



IKARUS security.manager Manual



IKARUS Security Software GmbH
Blechturmstraße 11
1050 Vienna
Austria

© IKARUS Security Software GmbH
www.ikarussecurity.com

Contents

1 Introduction	8
2 General information	9
2.1 The IKARUS security.manager Server	9
2.2 The IKARUS security.manager UI	10
3 Installation	11
3.1 Server-installation.....	11
3.1.1 System Requirements.....	12
3.1.2 Installation steps	13
3.2 UI-Installation	27
3.2.1 System Requirements.....	27
3.2.2 Installation steps	28
3.3 Upgrading an IKARUS Security Manager with Version < 4.0.....	34
4 Licensing	35
4.1 Registration	35
4.1.1 Activation Key	36
4.2 License Violation	37
5 Two different modes	39
5.1 Login	39
5.2 Single mode	40
5.2.1 Change-Management	41
5.3 Management mode.....	42
5.3.1 Managing multiple IKARUS security.manager (management mode)	44
6 The User Interface.....	45
6.1 Directory.....	45
6.1.1 Formatting.....	46
6.1.2 Window structure	46
6.1.3 Icons	51
6.1.4 Manual group.....	51
6.1.5 Multi-selection.....	52
6.1.6 Administering Groups.....	52
6.2 The main window	52
6.2.1 Global overview page.....	52

6.2.2 Overview Page.....	54
6.2.3 General Page.....	55
6.2.4 Properties Page.....	58
6.2.5 Charts Page.....	60
6.3 Footer Window	62
6.3.1 Pending Tasks	63
6.3.2 Virus List.....	66
6.3.3 Log File.....	68
6.3.4 Change Log	70
6.4 The Menu Bar.....	70
6.4.1 File Menu	71
6.4.2 View Menu	71
6.4.3 Tools Menu	72
6.4.4 Help Menu	87
6.4.5 Management Menu	89
6.5 The Toolbar	102
6.5.1 IKARUS anti.virus Configurations.....	102
6.6 Notification Bar	115
6.6.1 Layout.....	115
7 The Shared Directory	116
8 Software Distribution	117
8.1 Installing the IKARUS anti.virus.....	117
8.2 Uninstalling the IKARUS anti.virus.....	118
9 Configuration file	120
9.1 The <config> Section.....	121
9.2 The <ldap> Section	121
10 Glossary	123
11 Contact.....	127

List of figures

Figure 1 Server Installation – Installation of SQL Express Version	11
Figure 2 Server Installation – Installation of SQL Express Version	13

Figure 3 Server Installation – Welcome	14
Figure 4 Server Installation – License Agreement	15
Figure 5 Server Installation – User Settings.....	16
Figure 6 Server Installation – Network Settings	17
Figure 7 Server Installation – Database Settings	18
Figure 8 Server Installation – Administrator Information	19
Figure 9 Server Installation – LDAP Settings.....	20
Figure 10 Server Installation – Deployment Settings	21
Figure 11 Server Installation – Select Installation Folder	22
Figure 12 Server Installation – Confirm Installation.....	23
Figure 13 Server Installation – Add a license.....	24
Figure 14 Server Installation – Update product.....	25
Figure 15 Server Installation – Installation Complete.....	26
Figure 16 UI Installation – Choose language	27
Figure 17 UI Installation – Welcome	28
Figure 18 UI Installation – License Agreement	29
Figure 19 UI Installation – Port definition	30
Figure 20 UI Installation – Select Installation Folder	31
Figure 21 UI Installation – Confirm Installation.....	32
Figure 22 UI Installation – Installation Complete.....	33
Figure 23: UI – IKARUS security.manager Registration.....	36
Figure 24: UI – IKARUS security.manager License Activation.....	36
Figure 25: UI – License Violation	37
Figure 26: UI – Login to single mode	39
Figure 27: UI – Login to single mode	40
Figure 28: UI –Password definition (single mode).....	41
Figure 29: UI – Change Management.....	42
Figure 30: UI – Login to management mode.....	43
Figure 31: UI –Password definition (management mode)	44
Figure 32: UI – User Interface	45
Figure 33: UI – Directory (single mode)	46
Figure 34: UI - Directory Toolbar	47
Figure 35: The scan options	47
Figure 36: The context menu for actions on a client.....	48
Figure 37: The choice for administration or exclusion from administration	48
Figure 38: The Group/Client Tree.....	49
Figure 39: The Context-Menu for a Group/Client	50

Figure 40: The Tools Context Menu for a Client	50
Figure 41: UI – Directory Filter.....	50
Figure 42: UI – Global overview page.....	52
Figure 43: UI – Global overview page - shortcut menu	53
Figure 44: UI – Overview Page.....	55
Figure 45: UI – General Page on Groups	57
Figure 46: UI – General Page on Clients	58
Figure 47: UI – Properties Page	60
Figure 48: UI – Charts Page	62
Figure 49: UI – Pending Tasks	64
Figure 50: UI – Task Details	66
Figure 51: UI – Virus List	68
Figure 52: UI – Virus Information	68
Figure 53: UI – Log File	69
Figure 54: UI – Change Log	70
Figure 55: UI – Menu Bar – File Menu	71
Figure 56: UI – Menu Bar – View Menu	72
Figure 57: UI – Menu Bar – Tools Menu	73
Figure 58: UI – Clean host-entries from database	74
Figure 59: UI – IKARUS security.manager Settings – General	76
Figure 60: UI – IKARUS security.manager Settings – E-Mail Notifications.....	77
Figure 61: UI – IKARUS security.manager Settings – Reports	79
Figure 62: UI – IKARUS security.manager Settings – Update	81
Figure 63: UI – IKARUS security.manager Settings – Fileshare	82
Figure 64: UI – IKARUS security.manager Settings – LDAP.....	84
Figure 65: Charts options	86
Figure 66: PDF Report settings	87
Figure 67: UI – Menu Bar – Help Menu	88
Figure 68: UI – About Dialog	89
Figure 69: UI – Menu Bar – Management Menu	89
Figure 70: UI - "Management" menu, "Export configuration file" menu option.....	90
Figure 71: UI – Options dialogue	91
Figure 72: UI – Shortcut menu in the options dialogue	92
Figure 73: UI - Edit dialogue	93
Figure 74: UI - Edit dialogue, entering invalid data	94
Figure 75: UI - Edit dialogue, changing the password for a new installation.....	95
Figure 76: UI - Edit dialogue, checking the access data	96

Figure 77: UI - "Management" menu, "Export configuration file" menu option.....	97
Figure 78: UI - "Export configuration file" dialogue - selecting the ISM instances to be exported	98
Figure 79: UI "Export configuration file" dialogue - error message in the event of an invalid password. ...	99
Figure 80: UI "Export configuration file" dialogue - valid password	100
Figure 81: UI - Save file dialogue for exporting the configuration file	101
Figure 82: UI - Changing the password for management mode.....	101
Figure 83: UI – Toolbar.....	102
Figure 84: UI – IKARUS anti.virus Configurations.....	103
Figure 85: Configuration General Tab	104
Figure 86: Configuration e-mail tab.....	105
Figure 87: Configuration Update tab.....	106
Figure 88: Configuration Dial-Up Connections tab.....	107
Figure 89: "IKARUS anti.virus-Configurations" Exclusion tab.....	108
Figure 90: Configuration Exclusion tab (File exclusion)	109
Figure 91: Configuration Logs tab.....	110
Figure 92: Configuration Extras tab	111
Figure 93: Configuration Anti-Spam tab.....	112
Figure 94: Configuration Advanced Spam Protection	113
Figure 95: Configuration Scans tab	114
Figure 96: Configuration Add Scan Profile.....	115
Figure 97: UI – Notification Bar.....	115
Figure 98: Software Distribution – Installation process	118

List of tables

Table 1: Buttons for moving.....	38
Table 2: Overview Symbols.....	51
Table 3: Overview Symbols.....	57
Table 4: Task States - Symbols.....	65
Table 5: Possible settings for <config>.....	121
Table 6: Possible settings <ldap>.....	122
Table 7: Glossary.....	126

1

Introduction

Thank you for choosing the IKARUS security.manager, the simple and inspired solution that always provides the computers on your network with the latest virus and spam database updates and IKARUS anti.virus versions. Basically, IKARUS security.manager distributes the databases and updates from a central point to the computers on your network to save bandwidth, download volume, and, above all, administration time and costs.

2

General information

The IKARUS security.manager allows for installing, updating, uninstalling, and configuring the IKARUS anti.virus on your network.

The IKARUS security.manager consists of two separate applications: the IKARUS security.manager Server and the IKARUS security.manager UI. Both can be installed and run on different computers separately from each other. This separation allows you to control and maintain your network protection from anywhere and anytime you want.

2.1 The IKARUS security.manager Server

The IKARUS security.manager Server is the core of the IKARUS security.manager. It is the part that actually does all the distributional and statistical work and also handles the communication between the IKARUS security.manager and the IKARUS anti.virus installed on the computers on your network.

The IKARUS security.manager Server runs on a Windows server operating system as a service. All of the settings and information the IKARUS security.manager Server holds are saved in a MSSQL database, which can but does not need to reside on the computer where the IKARUS security.manager Server is installed. The communication between the IKARUS security.manager and the IKARUS anti.virus on your network is established via TCP using 9887 as the default port number. That port can be modified in the Configuration file of the IKARUS security.manager Server.

Since the IKARUS security.manager Server needs to perform executional tasks remotely on computers on your network, it needs appropriate rights. Therefore, we highly recommend installing the IKARUS security.manager Server service using a user account with administrative rights for your domain. This will ensure that the IKARUS security.manager Server is allowed to install and administer the IKARUS anti.virus on computers within the domain on your network. For further information about this topic and the administration of computers outside your domain, please read the Software Distribution chapter.

2.2 The IKARUS security.manager UI

The IKARUS security.manager UI provides the graphical interface to control the IKARUS security.manager Server. You can install the IKARUS security.manager UI on any computer you wish to control the IKARUS security.manager Server from. For more information about the layout and different windows of the IKARUS security.manager UI, refer to section 6.

Note: You must run the UI as an administrator; otherwise the update of the IKARUS security.manager UI to a later version might fail.

3

Installation

In this chapter, you will be guided through the installation process of the IKARUS security.manager. The setup is split into two separate installation processes: the IKARUS security.manager Server setup and the IKARUS security.manager UI setup. Both setup processes will automatically check your target system for installed prerequisites needed for the [application](#) to run and will optionally install missing software requirements automatically before the actual installation of the IKARUS product is started. Note that a restart of the target computer may be required during the installation of missing prerequisites. In this case, the setup process will automatically continue after a successful restart of the computer.

Note: To install the server and the UI you need administrative rights. If the User Access Control feature is enabled, launch setup using the Run as Administrator command.

3.1 Server-installation

To launch the installation of the IKARUS security.manager Server, double-click the Setup-ISM (server) xxxx file (where xxxx represents the version number).

After selecting your desired language the setup will be started automatically.

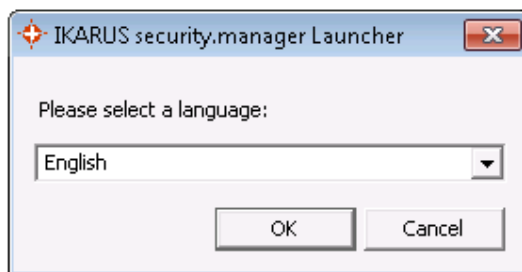


Figure 1 Server Installation – Installation of SQL Express Version

3.1.1 System Requirements

Hardware requirements:

- Processor from 2 GHz (Intel/AMD)
- 2 GB RAM
- display resolution min. 1024 x 768
- Diskspace for
 - ✓ server 2 GB
 - ✓ graphical user interface 20 MB
- Internet Connection (Updates)
- Active Directory (Microsoft domain structure)
- MSSQL database

Software Requirements:

- Client OS: Windows XP SP3 or higher
- Server OS: Windows server 2013 or higher

3.1.1.1 Firewall Settings:

Important: The communication (server and client side) between IKARUS security.manager and IKARUS anti.virus uses port 9888 by default.

The communication between IKARUS security.manager service and its graphical interface uses port 9887 by default.

These ports can be changed (see [6.2.14.1 General](#)) and has to be allowed by any kind of firewall as incoming and outgoing.

3.1.2 Installation steps

3.1.2.1 Select Microsoft SQL Express Version

The **IKARUS security.manager Server** needs a [MSSQL](#) database where it can store the settings, configurations and [client](#) information. The database can reside on the computer where the **IKARUS security.manager Server** will be installed to, but does not have to. Before installation will be started, please choose if you want to install a Microsoft SQL Express Version or if you already have an existing database.

If you do not have a local Microsoft SQL Version installed, then choose “Use existing database”. You have to setup a connection string later. But if you do not install within this dialog your Microsoft SQL Express instance and you want to use a local one, then you have to quit the setup because Microsoft SQL Express is a prerequisite.

You can choose to install a new “Microsoft SQL Express 2008 R2” or “Microsoft SQL Express 2012”, which are both free of charge, instance, or to use an existing one on the local machine or on a remote host (see Figure 2). If you choose to install a new instance the software must be downloaded from the internet, therefore you will need a working internet connection. Should something go wrong with the download process you may want to check the [proxy server](#) information you provided at the “[Network Settings](#)” dialog to ensure a working connection to the Internet.



Figure 2 Server Installation – Installation of SQL Express Version

3.1.2.2 Welcome

Click Next to read the license agreement.



Figure 3 Server Installation – Welcome

3.1.2.3 License Agreement

The licensing conditions must be accepted to install the **IKARUS security.manager Server**.



Figure 4 Server Installation – License Agreement

3.1.2.4 Service Log On Credentials

The **IKARUS security.manager Server** is installed as a [service](#). [Services](#) can be installed with the local system accounts or a user account within your [domain](#). Since the **IKARUS security.manager Server** needs appropriate rights to perform a binary execution remotely, it is highly recommended to install the **IKARUS security.manager Server** [service](#) with a user account which is allowed to administer the [domain](#).

If you choose “run service as LocalSystem” you can only proceed after checking if the given password and the username are correct otherwise next button will not be enabled.

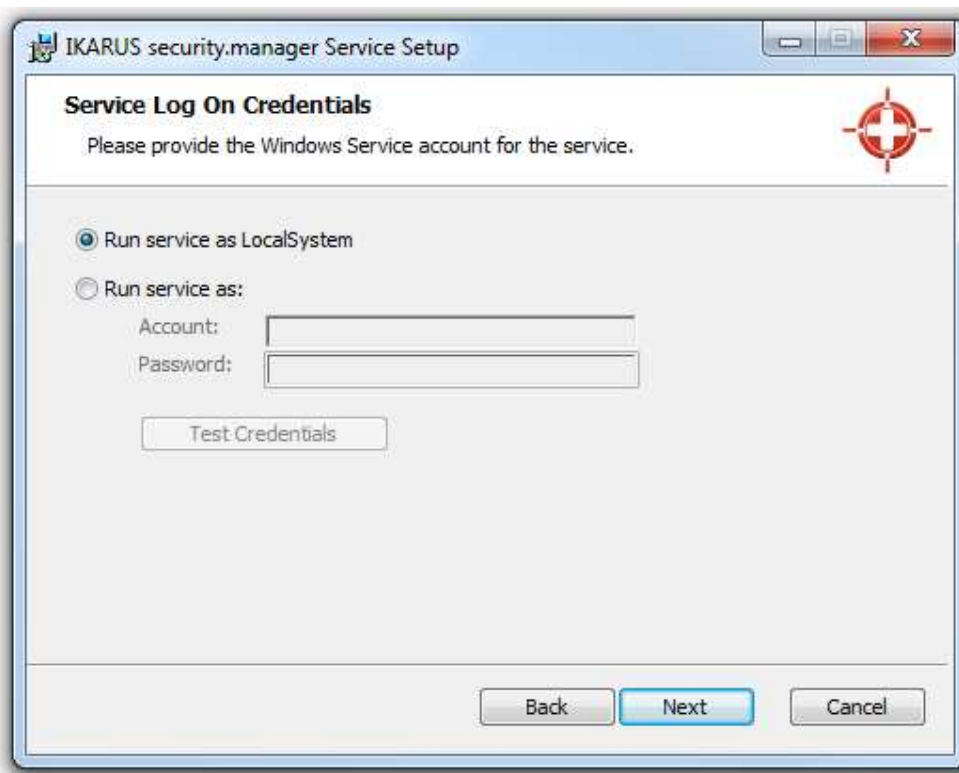
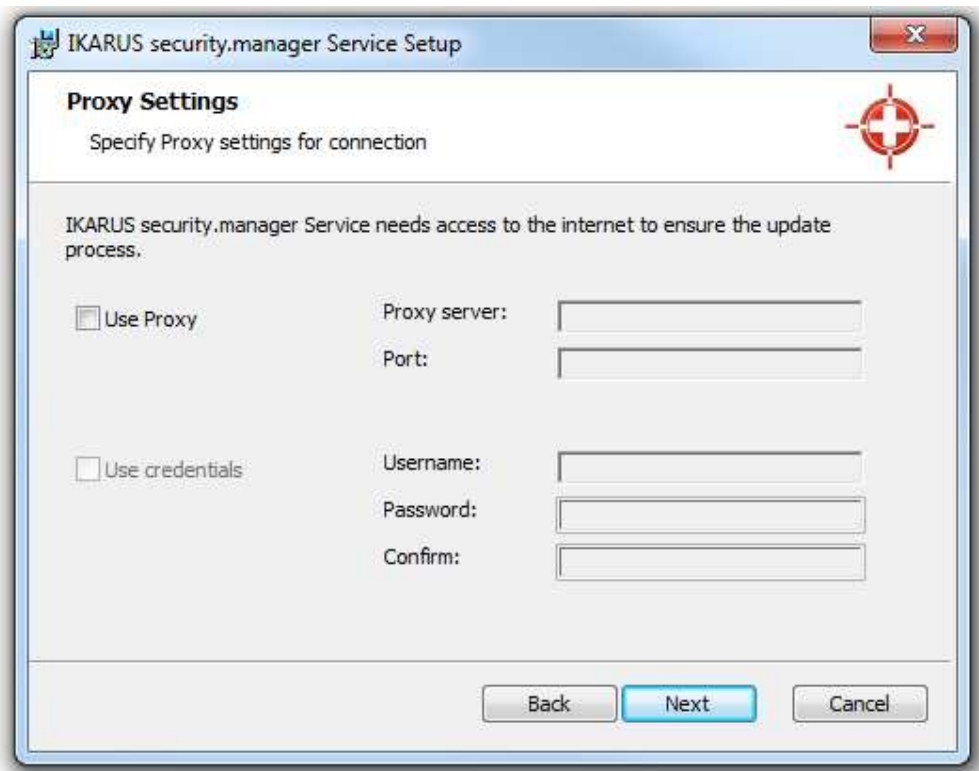


Figure 5 Server Installation – User Settings

Note: If you are using a **Windows Small Business Server (SBS)**, please make sure that you use the following format for the domain user credentials: **domain\user**. Windows SBS does not except credentials provided in the format user@domain.

3.1.2.5 Network Settings

If you have set up a [proxy server](#) for your Internet connection, you need to specify the correct settings for your [proxy server](#) to allow the **IKARUS security.manager Server** to access the Internet. The accuracy of the information you provide here is mandatory for an expedient use of the **IKARUS security.manager**. **No Internet access means** that **no updates** can be retrieved from the IKARUS update servers; thus, **your network will be open to possible threats**.



The image shows a Windows-style dialog box titled "IKARUS security.manager Service Setup". Inside, the "Proxy Settings" section is active, with the instruction "Specify Proxy settings for connection". A note states: "IKARUS security.manager Service needs access to the internet to ensure the update process." There are two checkboxes: "Use Proxy" and "Use credentials". To the right of "Use Proxy" are input fields for "Proxy server:" and "Port:". To the right of "Use credentials" are input fields for "Username:", "Password:", and "Confirm:". At the bottom are "Back", "Next", and "Cancel" buttons. The "Next" button is highlighted in blue.

Figure 6 Server Installation – Network Settings

3.1.2.6 Database Settings

If you want to specify a [MSSQL](#) database on another computer simply click on “Enter manually” (see Figure 7) and replace the “SERVER=.” string with “SERVER=SERVER_NAME”, where “SERVER_NAME” is to be replaced with the server name of the target computer where the [MSSQL](#) database resides.

In case you already have at least one [MSSQL](#) instance installed the setup will list you the installed instances from which you can choose one you want to use. In case of local Microsoft SQL Version, you can also enter a database user that has the appropriate rights. Please keep in mind that within the `ism.conf` the password will be saved as plain text.

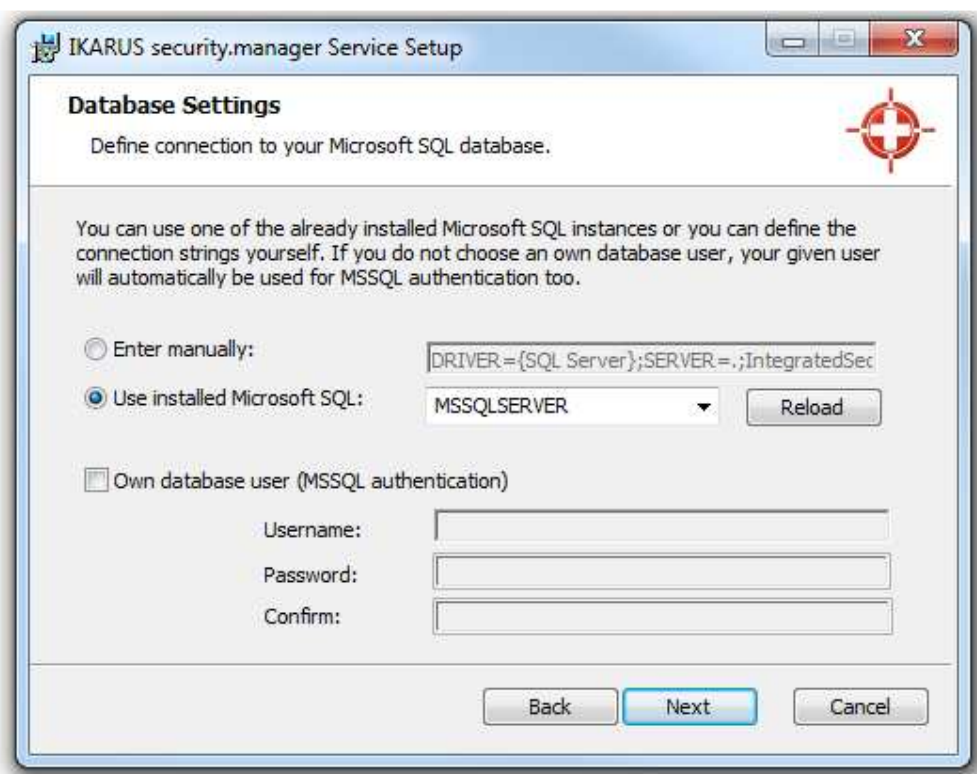
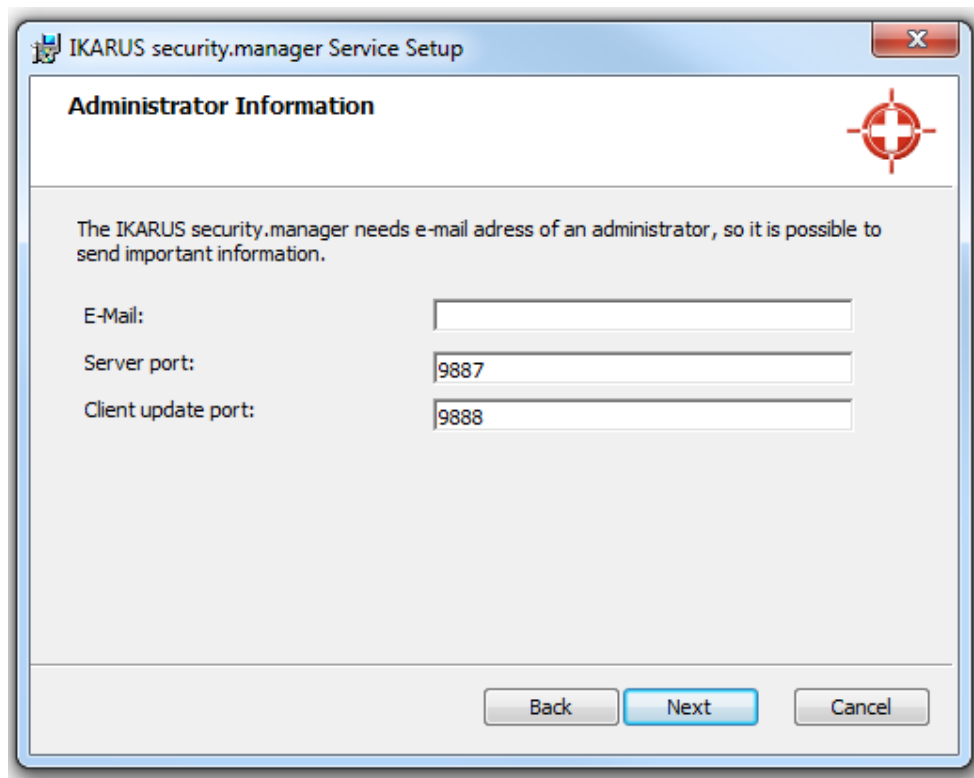


Figure 7 Server Installation – Database Settings

3.1.2.7 Administrator Information

In this dialog the **administrator's email address** has to be entered to enable sending of important e-mails in a later step. The **server port** defines a port where the **IKARUS security.manager UI can communicate with IKARUS security.manager Service**. **Client update** port is needed for doing the **update of the installed product**.



The dialog box is titled "IKARUS security.manager Service Setup" and "Administrator Information". It contains a text box explaining that the IKARUS security.manager needs an administrator's email address to send important information. Below this, there are three input fields: "E-Mail:" (empty), "Server port:" (containing "9887"), and "Client update port:" (containing "9888"). At the bottom, there are three buttons: "Back", "Next", and "Cancel".

Figure 8 Server Installation – Administrator Information

3.1.2.8 [LDAP](#) Settings

If the **IKARUS security.manager Server** setup is unable to automatically read out and provide the necessary information about your [LDAP](#) configuration, you may define the server name and credentials the **IKARUS security.manager Server** should use for communicating with the [LDAP](#) server.



The screenshot shows a Windows-style dialog box titled "IKARUS security.manager Service Setup". Inside, the "LDAP Settings" section is active, with the instruction "Specify LDAP settings for connection". A message states: "The IKARUS security.manager needs information about the LDAP it is connected to. Please provide the following information:". Below this, there are input fields for "Servername:" (containing "localhost"), "Credentials:" (containing "user@domain"), "Password:", and "Confirm:". A checkbox labeled "Login anonymously" is checked. At the bottom, there are "Back", "Next", and "Cancel" buttons.

Figure 9 Server Installation – LDAP Settings

3.1.2.9 Deployment Settings

To distribute the **IKARUS anti.virus** on your network, the **IKARUS security.manager Server** needs a place to store the binaries used for installing the **IKARUS virus.utilities**. For that purpose, you will need to set up (if you have not done so already) a [network share](#) where all [clients](#) you want to install the **IKARUS anti.virus** on have at least read access to. For further information about the **IKARUS anti.virus** deployment, refer to the [Software Distribution](#) and [Shared Directory](#) sections.

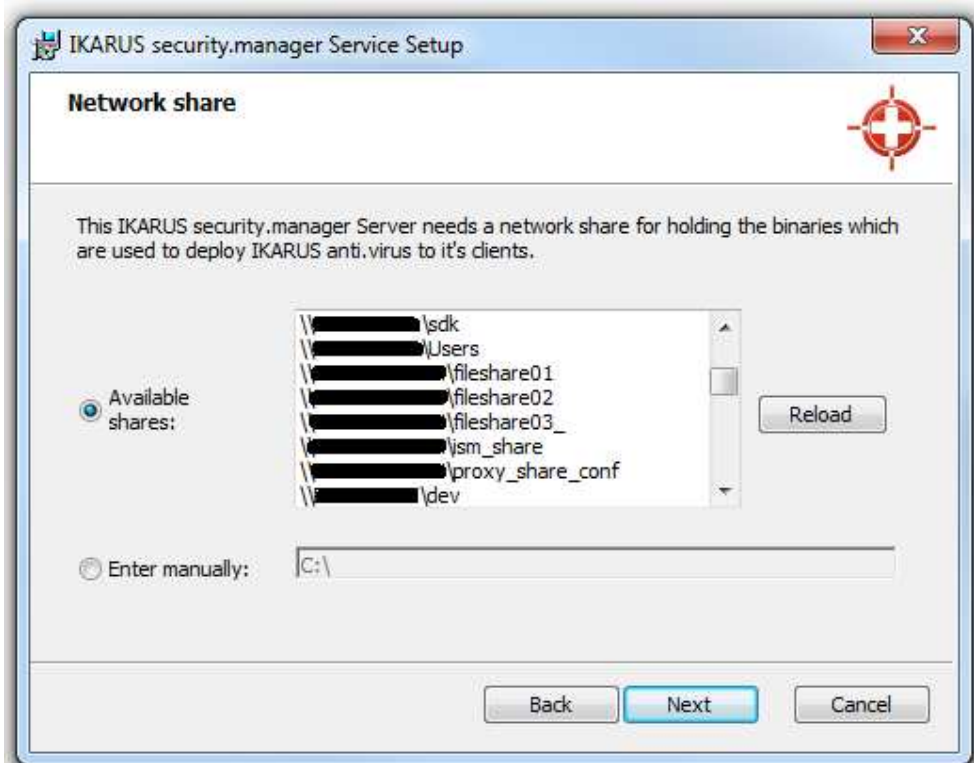


Figure 10 Server Installation – Deployment Settings

3.1.2.10 Selecting the Installation Folder

In this dialog, you can choose the destination folder to install the **IKARUS security.manager Server** files to.

The displayed folder is the basic folder within this folder the folder structure IKARUS\security.manager\service will be installed.



Figure 11 Server Installation – Select Installation Folder

3.1.2.11 Confirm Installation

This is the final step before the **IKARUS security.manager Server** files are actually installed. Click Next to start the copy process.



Figure 12 Server Installation – Confirm Installation

3.1.2.12 Add License

If a license is already available, it is possible to enter here. Otherwise by the help of “Purchase license” customers can buy a new license.

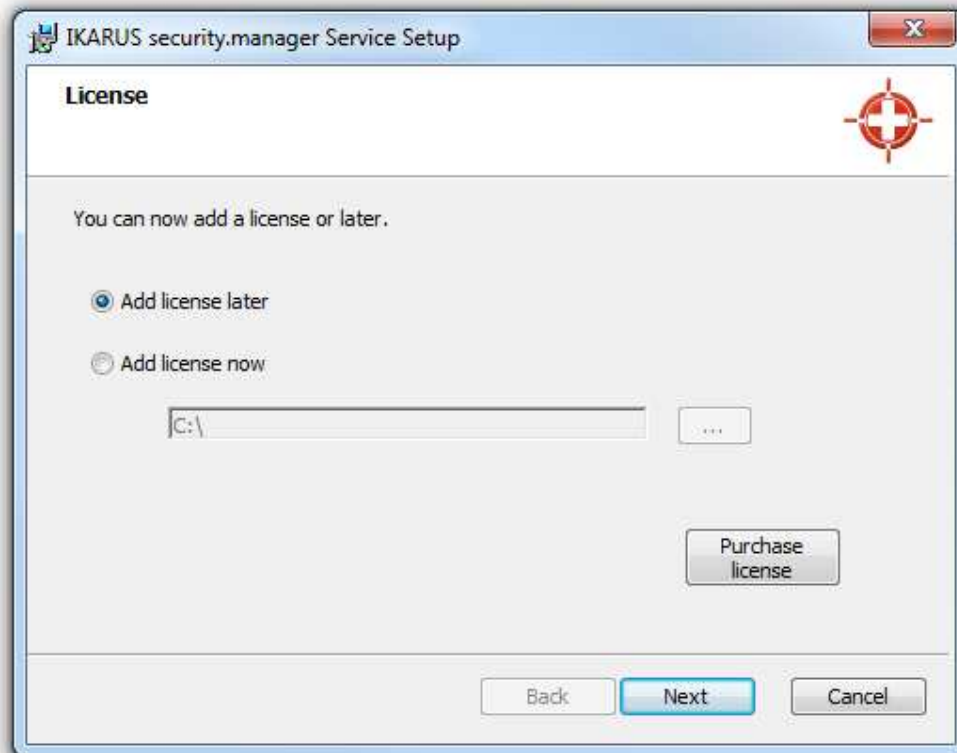


Figure 13 Server Installation – Add a license

3.1.2.13 Update Product

This is the last step of the **IKARUS security.manager Service setup**. After pressing next, the newest files will be downloaded but only if a license was added first. **IKARUS security.manager Service** will be initialized and the service will be started afterwards.

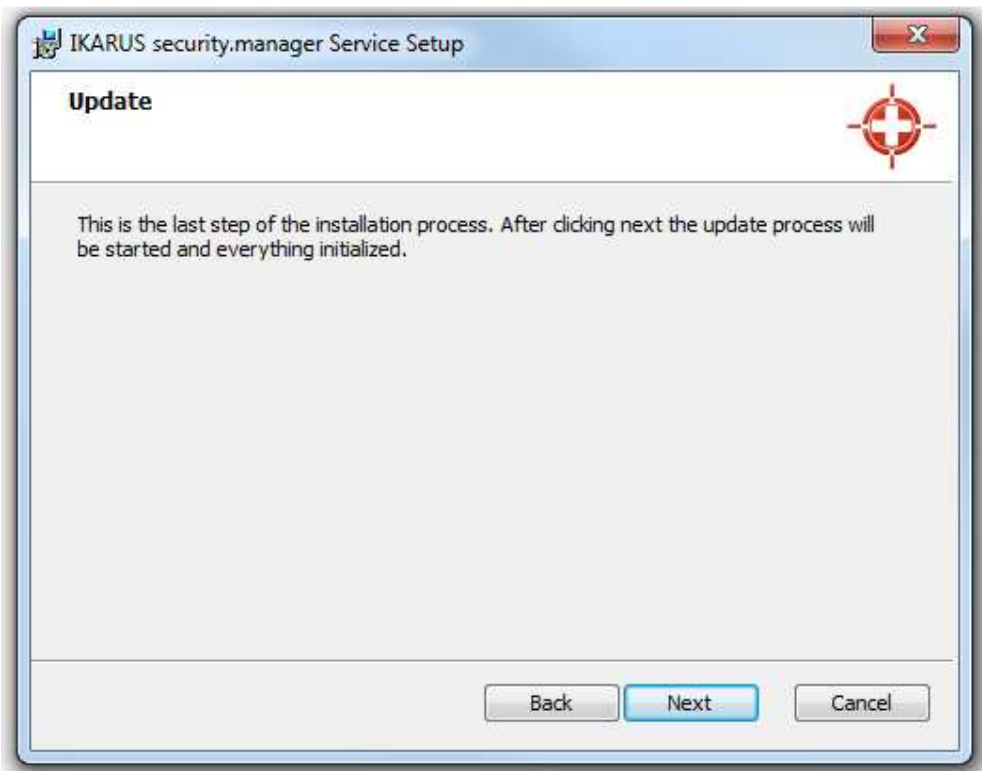


Figure 14 Server Installation – Update product

3.1.2.14 Installation Complete

Congratulations! You have successfully installed the **IKARUS security.manager Server**. If a different text is displayed in this dialog, contact the IKARUS support hotline.



Figure 15 Server Installation – Installation Complete

3.2 UI-Installation

To launch the installation of the IKARUS security.manager UI, double-click the Setup-ISM(UI)_xxxx file (where xxxx represents the version number).

After selecting your desired language the setup will be started automatically.

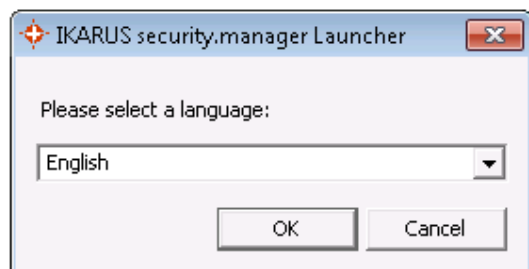


Figure 16 UI Installation – Choose language

3.2.1 System Requirements

Hardware requirements:

- Processor from 2 GHz (Intel/AMD)
- 2 GB RAM
- display resolution min. 1024 x 768
- Diskspace for
 - ✓ server 2 GB
 - ✓ graphical user interface 20 MB
- Internet Connection (Updates)
- Active Directory (Microsoft domain structure)
- MSSQL database

Software requirements:

- Windows Server 2012 (64 bit)
- Windows Server 2008, 32/64 Bit
- Windows Server 2008 R2, 64 Bit
- Windows 7, 32/64 Bit
- Windows Vista, 32/64 Bit
- Windows Server 2003, 32/64 Bit

3.2.2 Installation steps

Click Next to read the license agreement.



Figure 17 UI Installation – Welcome

3.2.2.1 License Agreement

The licensing conditions must be accepted to install the **IKARUS security.manager UI**.

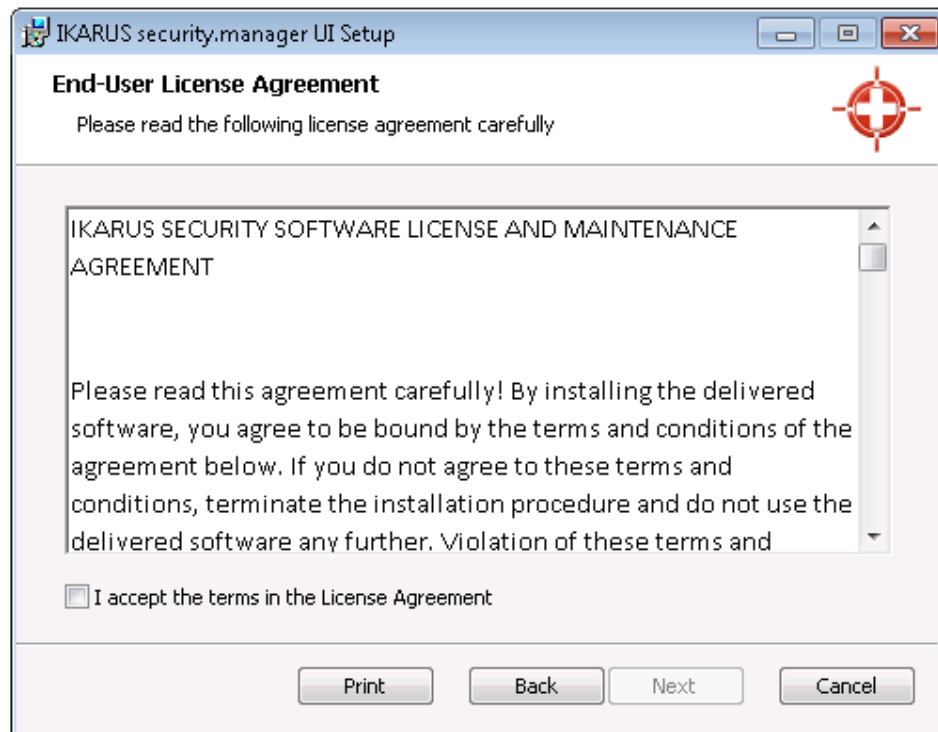


Figure 18 UI Installation – License Agreement

3.2.2.2 Selecting a port to connect to service

Before you proceed you have to select a port to connect to service later. The default value is 9887. Please keep in mind that this port is not blocked via a firewall.

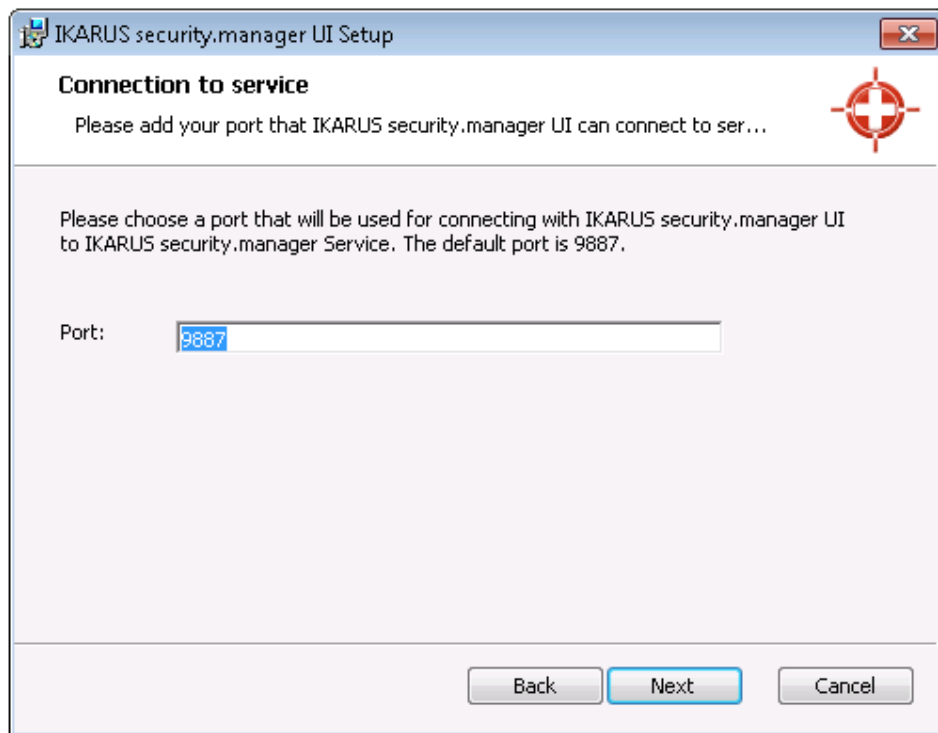


Figure 19 UI Installation – Port definition

3.2.2.3 Selecting the Installation Folder

In this dialog, you can choose the destination folder to install the **IKARUS security.manager UI** files to.

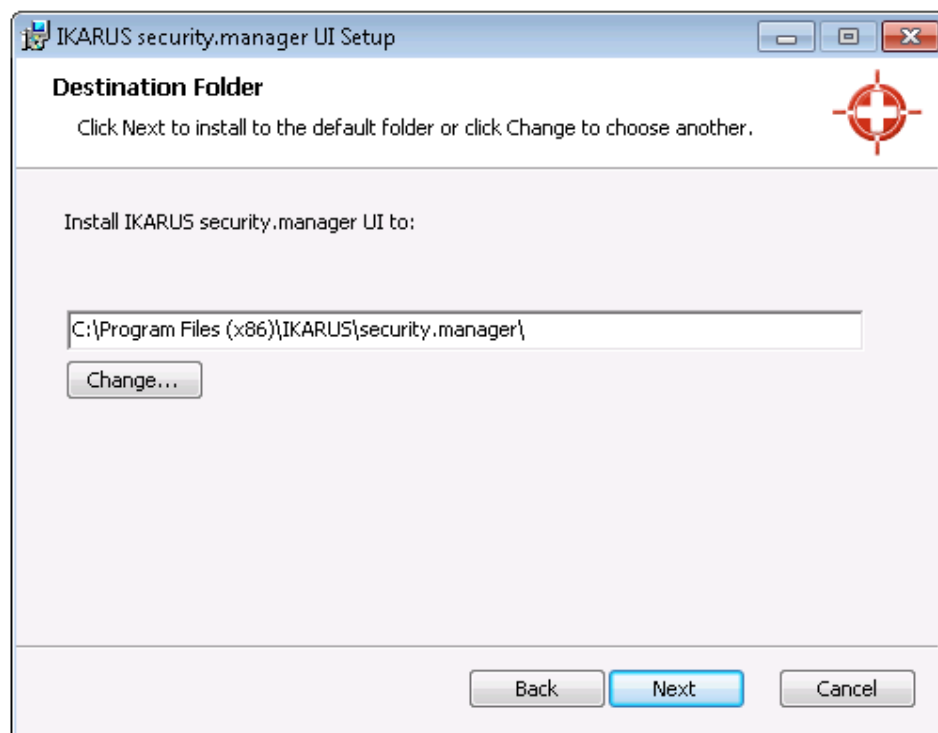


Figure 20 UI Installation – Select Installation Folder

3.2.2.4 Confirm Installation

This is the final step before the **IKARUS security.manager UI** files are actually installed. Click Next to start the copy process.

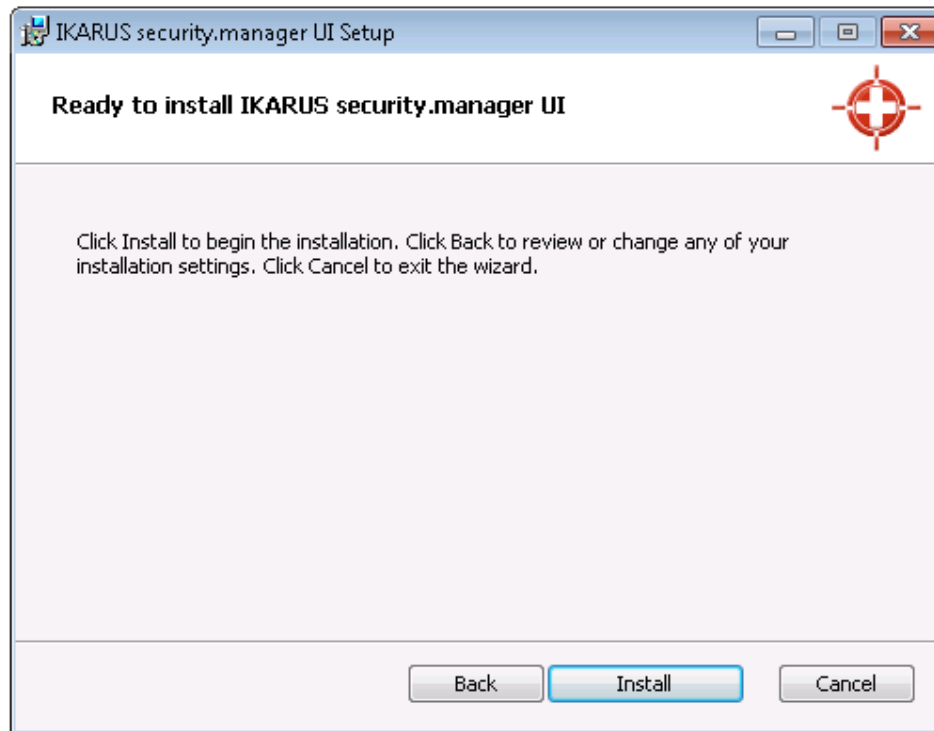


Figure 21 UI Installation – Confirm Installation

3.2.2.5 Installation Complete

Congratulations! You successfully installed the **IKARUS security.manager UI**. If a different text is displayed in this dialog, contact the IKARUS support hotline.

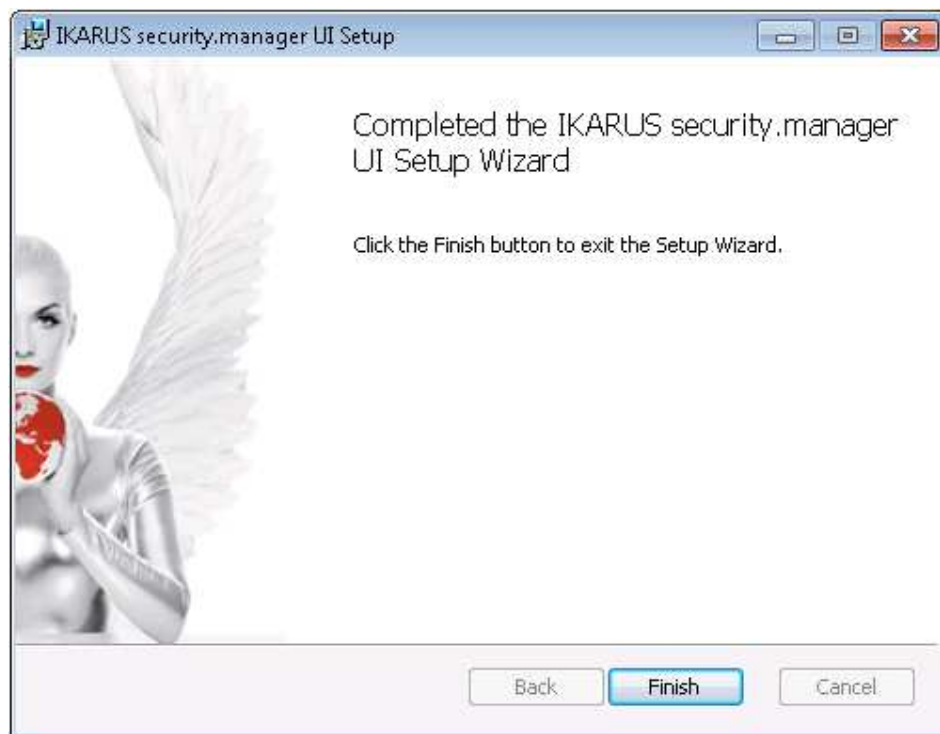


Figure 22 UI Installation – Installation Complete

3.3 Upgrading an IKARUS Security Manager with Version < 4.0

A legacy version of IKARUS Security Manager X (Version < 4.0) will automatically upgrade to the new IKARUS security.manager. (This requires enabling silent updates – see section 6.4.3.2.3.)

After the upgrade is complete, the installation path is unchanged but the directory structure contained in will have been rearranged, and binary filenames will have changed. Therefore, you might need to create new firewall rules as appropriate.

When the upgrade has been completed successfully, the database will assume the new structure and layout.

During the upgrade, a backup of your old database named ISMX_DATABASE_BACKUP.bak will be created in the log folder of your installation.

4

Licensing

To secure your network and operate the IKARUS security.manager, you will need a valid license. A license grants a defined amount of user licenses and should be selected appropriately for the size of your company. The IKARUS security.manager license is shared with all [clients](#) you need to administer. It is not possible to administer and run more IKARUS anti.virus instances on your network than the license allows. Licenses for non-administered [clients](#) (if you previously have bought one or more licenses for them) may exist; if not, you will not be able to administer any more [clients](#) after reaching the [client](#) limit of your IKARUS security.manager license. In this case, those particular clients will not be secured by the IKARUS anti.virus and will thus be unsecure. Remember that clients without a valid license are a possible threat to your entire network.

4.1 Registration

If there is no valid IKARUS security.manager license, the following dialog (Figure 23) will show up asking you to provide a valid license using an IKARUS license file or an [IKARUS Activation Key](#).

In the Registration dialog it is possible to choose one out of the following two options to register your IKARUS security.manager:

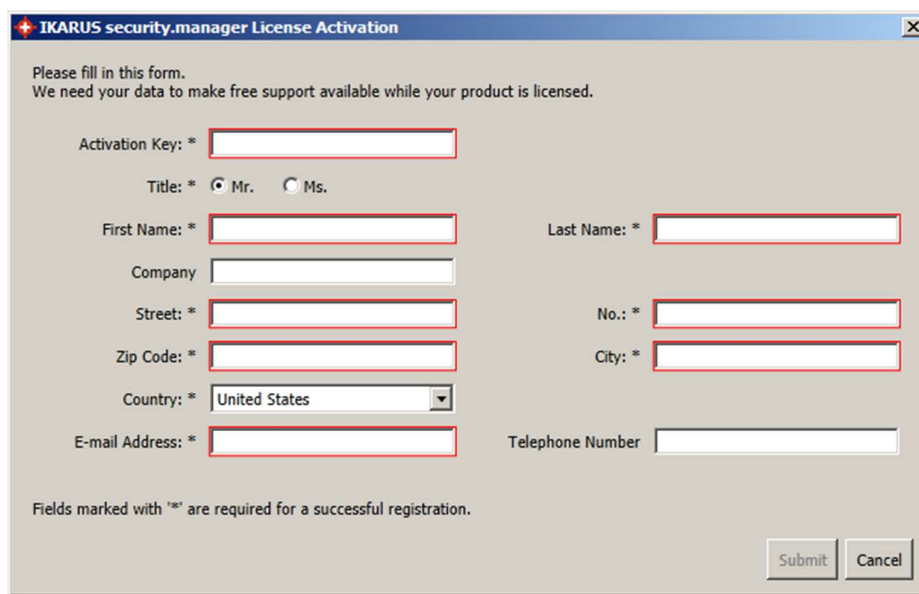
- License File: Opens a file browser where you can choose the IKARUS license file you want to use.
- Activation Key: Opens the activation window, see section 4.1.1.



Figure 23: UI – IKARUS security.manager Registration

4.1.1 Activation Key

If you have an [IKARUS Activation Key](#) rather than IKARUS license file, you may obtain a valid license from the License Activation window (Figure 24). Provide the requested information and submit your data. Upon successful submission of your data, you will get an e-mail with your license file attached to the specified address. All fields that have an asterisk are obligatory.



The dialog box titled "IKARUS security.manager License Activation" contains the following text:

Please fill in this form.

We need your data to make free support available while your product is licensed.

Activation Key: *

Title: * ☒ Mr. ☐ Ms.

First Name: * Last Name: *

Company

Street: * No.: *

Zip Code: * City: *

Country: *

E-mail Address: * Telephone Number

Fields marked with "*" are required for a successful registration.

Buttons: Submit, Cancel

Figure 24: UI – IKARUS security.manager License Activation

4.2 License Violation

If you do not have chosen a valid license file during the setup of the IKARUS security.manager Server, you will now be prompted again to either choose a license file or complete the registration using an [Activation Key](#).

There are a number of reasons why there are more [administered](#) clients on your network than actually allowed. This is a license violation, which is handled since version 4.0 of the IKARUS security.manager. You will be prompted to remove the excessive number of clients from [administration](#) to meet the requirements of the license you are using.

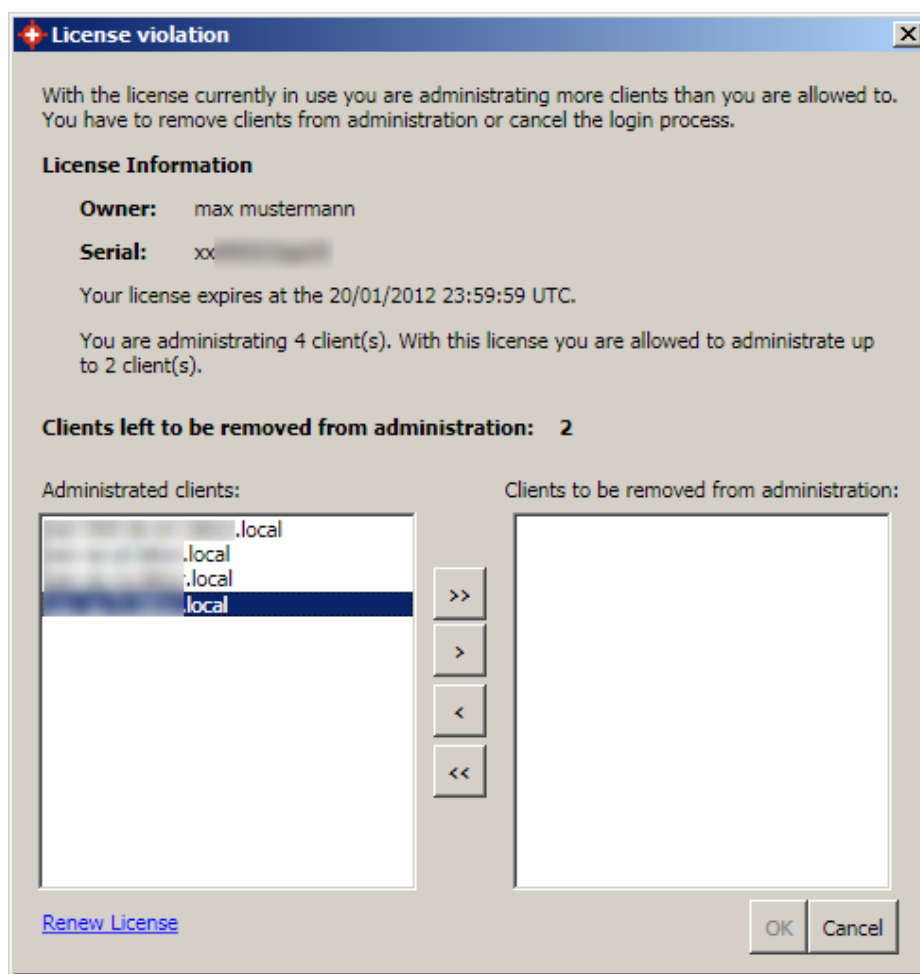


Figure 25: UI – License Violation

License Information:

Displays the expiration date and how much of your license capacity is used and free.

- Clients left to be removed from administration: Shows how many clients you need to remove from administration.





Button	Description
	Move all clients to the right-hand list.
	Move selected clients to the right-hand list.
	Move selected clients to the left-hand list.
	Move all clients to the left-hand list.

Table 1: Buttons for moving

- Administrated clients:
List of all clients that are administrated.
- Clients to be removed from administration:
List of all clients that will be removed from administration.
- Renew License:
Opens the registration window, see section 4.1.

The OK button applies all changes. This button is only enabled when you choose an appropriate number of clients. You may cancel this process but you will not be allowed to login to the IKARUS security.manager UI until you solve this issue. The clients will still be administered and protected by the IKARUS security.manager Server if you cancel this process.

If you need to purchase new licenses or have any questions concerning your license, please feel free to contact our sales team at sales@ikarus.at.

5

Two different modes

5.1 Login

When the IKARUS security.manager UI starts, the first thing that appears is the login dialog box, which offers two different modes:

- Single mode ("Login to management mode" not activated)
- Management mode ("Login to management mode" activated)



The image shows a screenshot of the IKARUS security.manager login dialog box. The window has a title bar with the text "IKARUS security.manager" and a close button. The main area features the IKARUS logo and the text "security.manager" in a large, bold, red font. Below this, there are four input fields: "Username" with the value "admin", "Password" with four dots, "Server" with a dropdown menu showing "localhost", and "Port" with the value "9887". At the bottom left, there is a checkbox labeled "Login to management mode" which is currently unchecked. To the right of the checkbox are two buttons: "OK" and "Cancel". At the very bottom of the dialog, there is a status bar with the text "Status: Login to ISM Server".

Figure 26: UI – Login to single mode

5.2 Single mode

In this mode, it is possible to manage a specific IKARUS security.manager. Therefore, some menu options that are supported in management mode are not active (see chapter 6.4.5). The login process must be carried out again in order to connect to another IKARUS security.manager.

During the login, you will be requested to enter your login information and specify the server to which you would like to establish a connection (this means the server on which the IKARUS security.manager server is installed). The TCP standard port through which connections are established is 9887 for communication between the IKARUS security.manager server and the IKARUS security.manager UI and 9888 for communication between the IKARUS security.manager server and IKARUS anti.virus clients. You can change these ports using the Options dialogue of the IKARUS security.manager UI. Please keep in mind that you might have to update also your firewall settings.

Single mode is useful for customers who only want to use one IKARUS security.manager-Server instance.



The image shows a Windows-style dialog box titled "IKARUS security.manager". The dialog has a red header bar with the IKARUS logo and the text "security.manager" in large red font. Below the header, there are four input fields: "Username" with the text "admin", "Password" with four dots, "Server" with a dropdown menu showing "localhost", and "Port" with the text "9887". Below these fields, there is a checkbox labeled "Login to management mode" which is currently unchecked. To the right of the checkbox are two buttons: "OK" and "Cancel". At the bottom of the dialog, there is a red status bar with the text "Status: Login to ISM Server".

Figure 27: UI – Login to single mode



Figure 28: UI –Password definition (single mode)

*When you login for the first time, you do not have a password yet.
Therefore simply leave the Password field free and click on the OK button.
You will be prompted to enter a new password for the specified user.*

5.2.1 Change-Management

If the option Ask for Request for Change-ID (RFC) is activated in the settings of the IKARUS security.manager server (see section 6.4.3.2), then you will be requested to give an RFC-ID in the login window. If the option Ask for a comment in the login screen (see section 6.3.4) is activated, then you will be prompted to enter a comment each time you try to login. This is useful, for example, if you are tracking changes to the settings or if you would like to explain the actions planned for the subsequent session.

IKARUS security.manager

IKARUS
security.manager

Username

Password

Server

Port

Request for Change ID

Comment

OK Cancel

Status: A comment is obligatory. Leading and trailing white spaces are ignored!

Figure 29: UI – Change Management

5.3 Management mode

The basic difference from single mode is that it is possible to change between different IKARUS security.manager servers without performing another login process by the help of the login window. More information on changing between IKARUS security.manager servers can be found in section 6.1. Furthermore, the login process also changes for management mode. The login information for the individual IKARUS security.manager servers must be given at a later time (see section 5.3.1).



The image shows a Windows-style application window titled "IKARUS security.manager". The window has a red header bar and a red footer bar. The main content area is white and contains the IKARUS logo and the text "security.manager" in a large, bold, red font. Below this, there are four input fields: "Username" with the value "admin", "Password" (empty), "Server" with the value "localhost", and "Port" with the value "9887". There is a checkbox labeled "Login to management mode" which is checked. To the right of the checkbox are two buttons: "OK" and "Cancel". At the bottom of the window, in the red footer bar, the text "Status: Login to ISM Server" is displayed.

IKARUS security.manager

IKARUS
security.manager

Username

Password

Server

Port

☒ Login to management mode

OK Cancel

Status: Login to ISM Server

Figure 30: UI – Login to management mode

Figure 31: UI –Password definition (management mode)

Any password can be chosen. It does not depend on an IKARUS security.manager server. This password is used to encrypt the settings file for management mode, which contains the desired IKARUS security.manager data.

5.3.1 Managing multiple IKARUS security.manager (management mode)

After a password has been created for the settings file, the data of the desired IKARUS security.manager-Server has to be added (see section 6.4.5.1). Additional information on how the password can be set for new installations can also be found in that section.

6

The User Interface

The layout of the IKARUS security.manager UI can be customized. Each window can be docked or undocked and moved anywhere on the screen. The window layout will be stored upon closing the IKARUS security.manager UI.

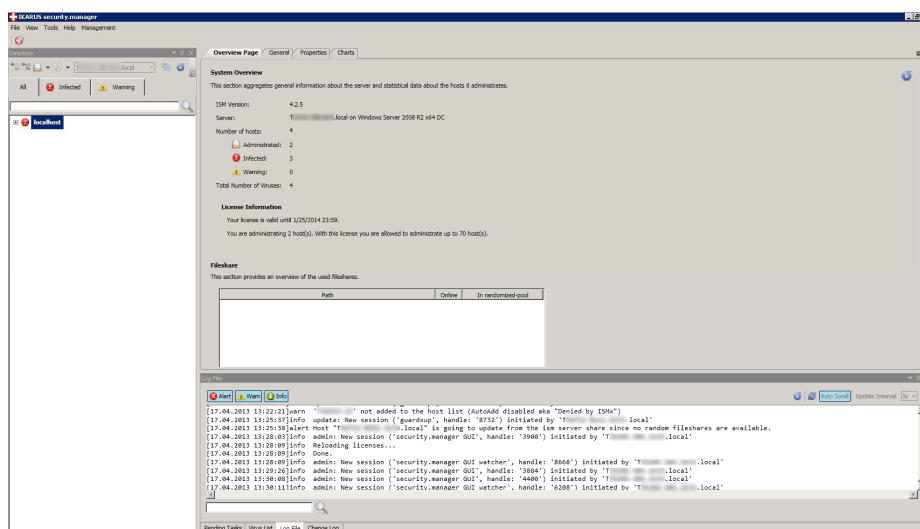


Figure 32: UI – User Interface

6.1 Directory

The Directory is the center of almost all [client](#) related operations. It holds the [clients](#) of your [Active Directory](#) and the [clients](#) you manually add (e.g. [clients](#) that exist outside your [domain](#) or in a different [domain](#)). All [clients](#) in the [Active Directory](#) are automatically listed with their [FQDN](#). It is highly recommended to always specify the [FQDN](#) of manually added [clients](#) – [clients](#) with the same name might exist in different [domains](#) and there is no way to distinguish between them.

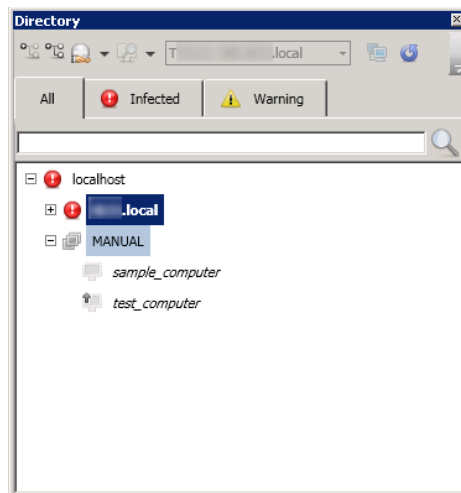


Figure 33: UI – Directory (single mode)

The directory window contains three sections. In the upper section the toolbar (see Figure 34) and in the middle section the Group/Client tree (see Figure 38). In the lowest section is the Filter section (See Figure 41), where the tree can be searched for clients or groups. The tree has also filters for clients with warning messages or infected clients.

6.1.1 Formatting

Node names are formatted depending on their respective status:

- **Normal:**
This client is online.
- *Italic:*
This client is offline.
- **Bold:**
This node is selected.

6.1.2 Window structure

The [Directory](#) is separated into the following three sections:

- Toolbar
- Group/Client Tree
- Filter Section

6.1.2.1 The Toolbar



Figure 34: UI - Directory Toolbar

The symbols described from left to right mean the following:

- Collapse all group nodes.
- Expand all group nodes.
- Opens the context menu for actions on the currently selected client (See Context Menu in this section).
- Scan options, see next figure.
- Chooses current connected IKARUS security.manager instance (check “change current IKARUS security.manager instance” in this section)
- Connect again to the current selected IKARUS security.manager instance. (see “reconnect” in this section)
- Refresh the directory.



Figure 35: The scan options

Fast System Scan:

Scans the windows directory and active processes (Only on currently selected client).

System Partition:

Scans the system partition (Only on currently selected client).

Entire Computer:

Scans the entire system (Only on currently selected client).

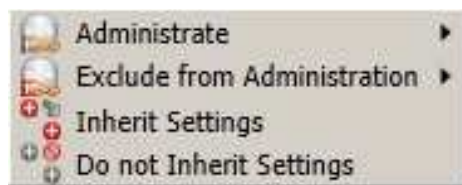


Figure 36: The context menu for actions on a client

The Context menu: shows all entries of the context menu that is available by clicking right mouse-button.

Administrate/Exclude from Administration: This context menu entry is also split up in further entries:

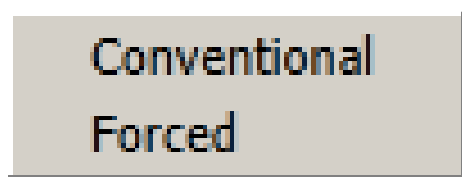


Figure 37: The choice for administration or exclusion from administration

- Administrate/Exclude from administration:
Allows/prevents updates and system protection.
- Administrate/Exclude from administration forced:
Ignores administration from another IKARUS security.manager.

Inherit Settings/Do not Inherit Settings:

Settings are taken/not taken from the parent node.

Change current IKARUS security.manager instance:

The main feature of the version 4.2.x is the management of more than one IKARUS security.manager-Servers. This is now possible by choosing the IKARUS security.manager-Server within the selection-box. The selection-box is shown only in management-mode. Single-mode uses automatically the IKARUS security.manager-Server which is entered in login-window.

Reconnect:

This action is only possible when no connection to the current selected IKARUS security.manager-Server is established. If the connection may not work, please verify your connection settings. For editing use options in management-mode-menu.

6.1.2.2 The Group/Client Tree

In the Group/Client tree the main node is always the first node in the tree (named "All"). This and all other nodes that have the same symbol in front of it are group nodes.

Nodes that have a computer monitor in front of them are client nodes (e.g.: node with the name "manual computer").



Figure 38: The Group/Client Tree

When an item is right-clicked with the mouse the context menu is opened. In the following figure all possible context menu entries are shown, but not all are always available. The first four in the context menu (Add Group, Add Computer, Delete and Rename) are only available for manually added groups/clients. The other entries are all shown when a group or a host is selected. Please keep in mind that the data-estimation might take some time. This leads to the fact that the data might not be immediately shown correctly after applying some changes.



Figure 39: The Context-Menu for a Group/Client

6.1.2.2.1 The Tools Context Menu

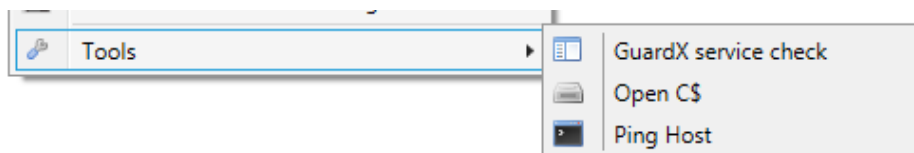


Figure 40: The Tools Context Menu for a Client

The 'Tools' context menu offers commands to check the connectivity of a host:

- GuardX service check: Tries to reach the GuardX service on the selected host.
- Open C\$: Opens C\$ of the selected host. This might require special user credentials.
- Ping Host: Sends a ping-command to the selected host and shows the result.

6.1.2.3 The Filter Section

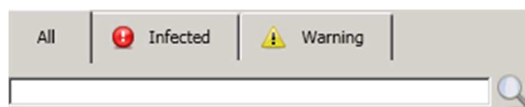


Figure 41: UI – Directory Filter

In the filter section of the directory a filter can be defined in a text box. This applies a case-insensitive filter by name. Only nodes that meet the filter criteria will be displayed. With the magnifying glass the next element matching the filter is selected.

The predefined tab filters are (see figure above):

- All (active):
Overview of all clients in your directory and all manually added clients.
- Infected (inactive):
Overview of all clients that are infected.
- Warning (inactive):
An overview of all outdated clients, i.e. clients with a virus database, spam database (should spam detection be enabled) and anti.virus update being older than 2 weeks. Also includes clients that are administrated and online but do not execute IKARUS anti.virus or cannot be reached by the IKARUS security.manager.

6.1.3 Icons

The icons of the nodes in the [Directory](#) provide a quick overview of the node statuses.









Symbol	Description
	This node is a group.
	This client is offline.
	This client is online and has no IKARUS anti.virus installed.
	This client is online, has the IKARUS anti.virus installed, and is administered.
	This client is online, has the IKARUS anti.virus installed, and is not administered.
	(Overlaid) This node inherits settings from its parent.
	(Overlaid) This node or one of its children is infected.
	(Overlaid) This node or one of its children is outdated or administered but unreachable.

Table 2: Overview Symbols

6.1.4 Manual group

The Manual group (displayed as MANUAL in the [directory](#)) is the bottommost group node in the root (All) node of the [directory](#). If you want to add computers from other [domains](#) or no [domain](#) at all, this is the place to do so. You can add, rename, remove, and move nodes ([clients](#) and groups).

6.1.5 Multi-selection

You can select multiple nodes by holding the Ctrl key on your keyboard while clicking. Consider that a multi-selection of a temporary group node does not exist anymore when multi-selection is cancelled (e.g. by simply selecting a single item). Actions and views available for group nodes are also available for a temporary group.

6.1.6 Administering Groups

If you administer a group, all children (clients and subgroups) will inherit from that group and binary updates will be automatically allowed for each client. All clients within the group where the IKARUS anti.virus are installed will be administered by your IKARUS security.manager.

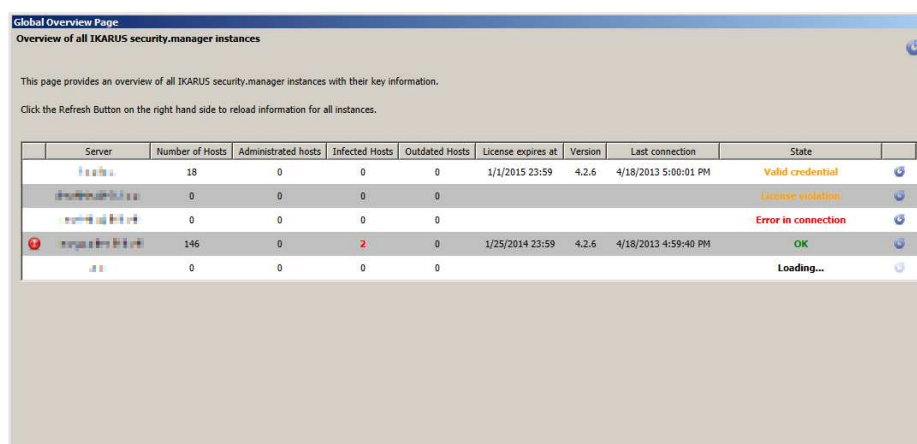
6.2 The main window

The main window is separated in 5 tabs:

- Global overview page
- Overview page
- General
- Properties
- Charts

6.2.1 Global overview page

This screen is used as an overview of all registered IKARUS security.manager servers, which is only available in management mode. The most important information is shown like the number of computers, how many computers are being administrated or are infected or not up-to-date. Furthermore, the current license, version and time stamp in connection with the last update are shown.










Server	Number of Hosts	Administrated hosts	Infected Hosts	Outdated Hosts	License expires at	Version	Last connection	State
	18	0	0	0	1/1/2015 23:59	4.2.6	4/18/2013 5:00:01 PM	Valid credential
	0	0	0	0				License violation
	0	0	0	0				Error in connection
	146	0	2	0	1/25/2014 23:59	4.2.6	4/18/2013 4:59:40 PM	OK
	0	0	0	0				Loading...

Figure 42: UI – Global overview page

The data of IKARUS security.manager servers is not updated automatically. The most recently retrieved connection data is saved and is available for the next login. Each IKARUS security.manager server can be updated individually by clicking  in the respective line. The  symbol on the top right can be used to update all entries in the global overview page.

After each update, the current status is provided, which gives information on possible problems:

- **Loading...**
The data is being retrieved.
- **OK**
The information was loaded successfully.
- **Error in connection**
The connection could not be established.
- **Valid credentials**
The access data is valid
- **License violation**
There was a problem with the license, which should be clarified.
- **The last connection was established more than two days ago**
- **No connection has never been established**

If a version is being used that is older than 4.2.x, then that IKARUS security.manager server cannot be used with management mode. Nevertheless, they are shown in the global overview page.

Furthermore, it is possible to use the right mouse button to call up the shortcut menu with the following entries.



Figure 43: UI – Global overview page - shortcut menu

- **Connect to service**
Changes to the currently selected IKARUS security.manager server and closes the connection to the previously selected IKARUS security.manager server.
- **Set to default ISM.**
The currently selected IKARUS security.manager server is set to be the default server after a restart.
- **Add**
Add a new IKARUS security.manager server to list. See chapter 6.4.5.1.2.

- **Edit**
The login properties of the currently selected IKARUS security.manager server are edited. The edit dialogue is not available if the selected IKARUS security.manager already has a connection to it or a connection is currently being established. See chapter 6.4.5.1.1.
- **Delete**
The currently selected IKARUS security.manager server is deleted permanently from the management list. Therefore it is no longer possible to establish a connection. The currently connected or default IKARUS security.manager server cannot be deleted from the list.

6.2.2 Overview Page

The Overview Page window (Figure 44) aggregates general information on the IKARUS security.manager Server and statistical information on the [clients](#) in the [Directory](#) as well as the added [fileshares](#) and their online/offline-states.

6.2.2.1 Layout

The overview page can be refreshed with the refresh button placed in the upper right corner and consists of the following sections:

- **Server information:**
Displays information about the IKARUS security.manager Server version and the host it is running on
- **Quick client overview:**
Provides a quick overview of all clients in the directory
- **License Information:**
Displays the expiration date and how much of your license capacity is used and free.
- **File share Information:**
Displays information of online/offline file shares.
- **Update Overview:**
Provides a quick overview of the version numbers the IKARUS security.manager Server has ready to deploy to its clients.

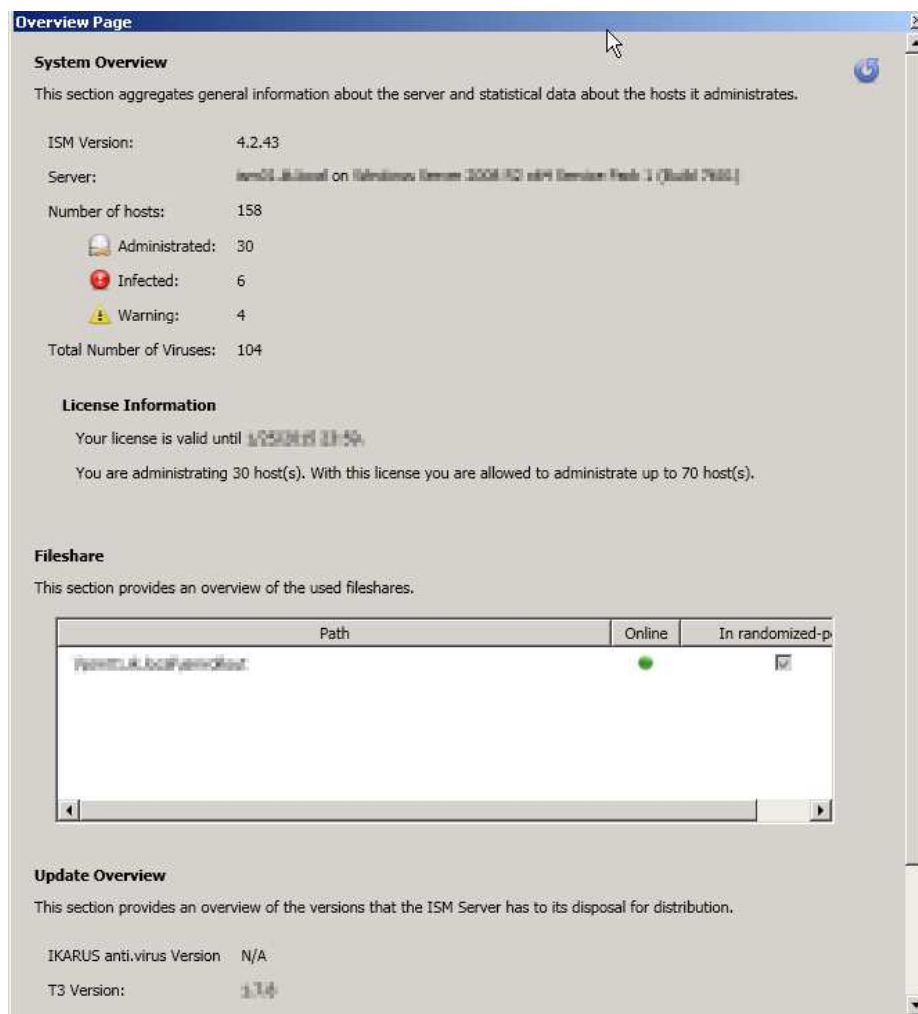


Figure 44: UI – Overview Page

6.2.3 General Page

6.2.3.1 General Page on Groups

The General Page window (Figure 45) on groups displays statistical information about [clients](#) within the currently selected group node. It provides you with an easy way to investigate the status of multiple [clients](#) in one place. If you need to investigate the status of multiple [clients](#) that are not in the same group, you may use the [Multi-selection](#) feature of the [Directory](#).

6.2.3.1.1 Layout

The General page for groups' shows summed up information about all hosts that are part of this group. At the top of the page general information is shown, such as:

- Name of the group:

Shows the name and status icons of the current node.

- **Total Number of Viruses:**
Shows the total number of infections on the current node.
- **Number of Clients Online:**
Shows the total number of online clients on the current node.
- **Number of Clients Guarded:**
Shows the total number of guarded clients on the current node.
- **Administrated:**
Shows the total number of administrated clients on the current node.

In the clients list beyond the general information, all hosts of the group can be seen in more detail, with the following information:

- **Status Icon:**
Shows the status icons of this client.
- **Name:**
Shows the name of this client.
- **Infections:**
Shows the number of infections on this client.
- **Online:**
Shows the online status of this client.
- **Service Installed:**
Shows the service installation status of this client.
- **Administrated:**
Shows the administration status of this client.
- **Last Update:**
Shows the date in UTC of the last update process on this client.
- **Last Time Online:**
Shows the date (in UTC format) of the last time this client was online.

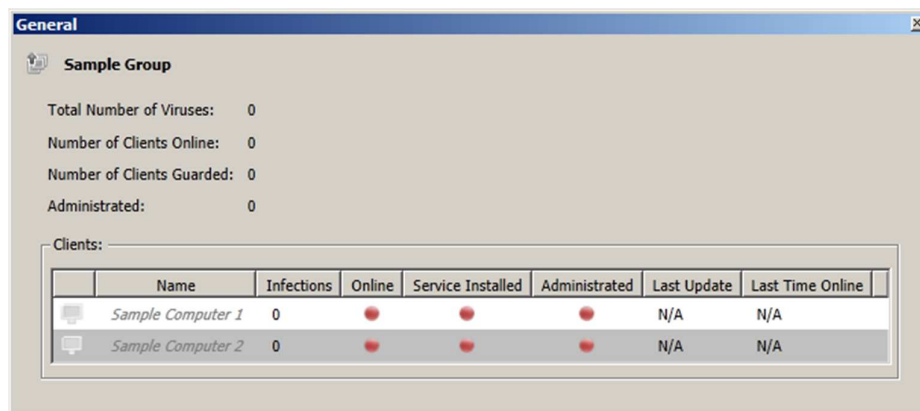


Figure 45: UI – General Page on Groups

6.2.3.1.2 Icons

Symbol	Description
●	Red icon means “No“
●	Green icon means “Yes“

Table 3: Overview Symbols

6.2.3.2 General Page on Clients

The General Page Window (Figure 46) of a [Client](#) displays detailed information on the currently selected [client](#).

6.2.3.2.1 Layout

The general page for clients is separated into informational sections. Those sections are:

- **General:**
Displays online, service installation and administration statuses of this client.
- **Update:**
Displays the time of the last update to this client and the date the next update process will occur.
- **Versions:**
Displays the IKARUS anti.virus, database, scan engine and update versions of this client.
- **Protection:**
Displays the serial number, scan status, number of infections and protection mechanisms that are enabled or disabled.



Figure 46: UI – General Page on Clients

6.2.4 Properties Page

The Properties Page window (Figure 47) provides a quick overview of the IKARUS anti.virus Configuration a [client](#) or group uses and when and how updates are issued for this [client](#) or group. You can set these settings [client](#)-wide or group-wide and let a group's [clients](#) inherit settings from the parent level. If you choose to inherit settings for a group, you will be asked if you also want the [clients](#) in that group to inherit the settings; on the contrary, if you choose to remove the inheritance settings of a group, you will be asked if you want to remove the inheritance settings from the [clients](#) in that group as well.

6.2.4.1 Update Section

In the Update Section, you can specify when and how updates are performed. It is possible to define per group or host one concrete [fileshare](#) that is always asked for an update. The default way for getting updates is a randomly chosen [fileshare](#) from the randomized-pool. [Fileshares](#) that are shown italic are at the moment offline. For further information about this topic, see section 6.4.3.2.4.

If you disallow binary updates, only virus and spam databases will be updated; the IKARUS anti.virus will not. If you for any reason want to hide the IKARUS anti.virus system tray status notifications (e.g. on a computer used for presentations where pop-up windows would otherwise distract the audience), enable the Disable system tray Status Notifications checkbox.

6.2.4.2 Language

In the Language Section, you can define in which language for IKARUS anti.virus should be set on the selected host. If you check “Overrule IKARUS anti.virus language settings”, the language you selected will be used in any case, otherwise the language can be set to a different value on the host itself.

6.2.4.3 Rights Management

The Rights Management section is useful for [clients](#) that are outside the [domain](#) of the IKARUS security.manager Server. Since the IKARUS security.manager Server needs appropriate rights to establish a connection and execute binaries remotely, you can specify credentials having the appropriate rights on this [client](#) to perform these operations.

6.2.4.4 Layout

At the top of the window is the name and status icon of the currently selected host or group shown. All other items on the window are described below:

- **Inherit Settings:**
Inherits/disinherits settings from the parent node. Inheritance is saved automatically e.g. you do not need to click the „Save” button.
- **IKARUS anti.virus Configuration:**
Sets the configuration this client is using.
- **Update Time:**
Choose the time span in which updates are performed.
- **Fileshare:**
Choose a concrete fileshare or take one from randomized pool if an update is necessary.
- **Allow Binary Updates:**
Allows updates to the IKARUS anti.virus binaries. Databases will still be updated if binary updates are disallowed.
- **Disable system tray Status Notifications:**
Prevents the IKARUS anti.virus tray status notifications to pop up.
- **Get Updates from External Servers:**
Allows IKARUS anti.virus to download updates from the Internet should the ISM be unable to provide updates.
- **Username/Password:**
Sets the credentials to be used for interaction with this client. If the client is not in the same domain as the ISM server, setting these credentials correctly is mandatory to ensure correct administrative behaviour on this client.
- **Browse Directory Group:**
Defines which Directory Groups are allowed to make some changes in IKARUS anti.virus.
- **Delete restriction:**
Removes a previously set Directory Group restriction.
- **Save Button:**
Saves these settings.
- **Cancel Button:**
Discards any changes made.

Figure 47: UI – Properties Page

6.2.5 Charts Page

The Charts Page shows the 5 standard charts that are currently available in the IKARUS security.manager and those 5 charts can be edited in the IKARUS security.manager options (see section 6.4.3.2.6).

The 5 standard charts are:

- Administration of Hosts,
- Availability of Hosts,
- Infection of Hosts,
- Virus Top 5 and

- Virus per Operating System.

In the page not only the charts are displayed, but also the time of creation. The charts can easily be refreshed by pressing the refresh button in the upper right corner.

The button to the left of the refresh button is used to create a PDF report of the charts. This report only holds all charts that were currently displayed in the Chart Page. The PDF report can also be adapted in the IKARUS security.manager options.

Note: You need to have a PDF viewer installed to view the PDF report.

For further information on how the charts can be edited and adapted go to the IKARUS security.manager options (see 6.4.3.2).

For displaying charts at least Internet Explorer Version 7 must be installed. To ensure full functionality it is recommended to use Internet Explorer Version 9. Consider to enable JavaScript because this is used for estimating charts.

6.2.5.1 Layout

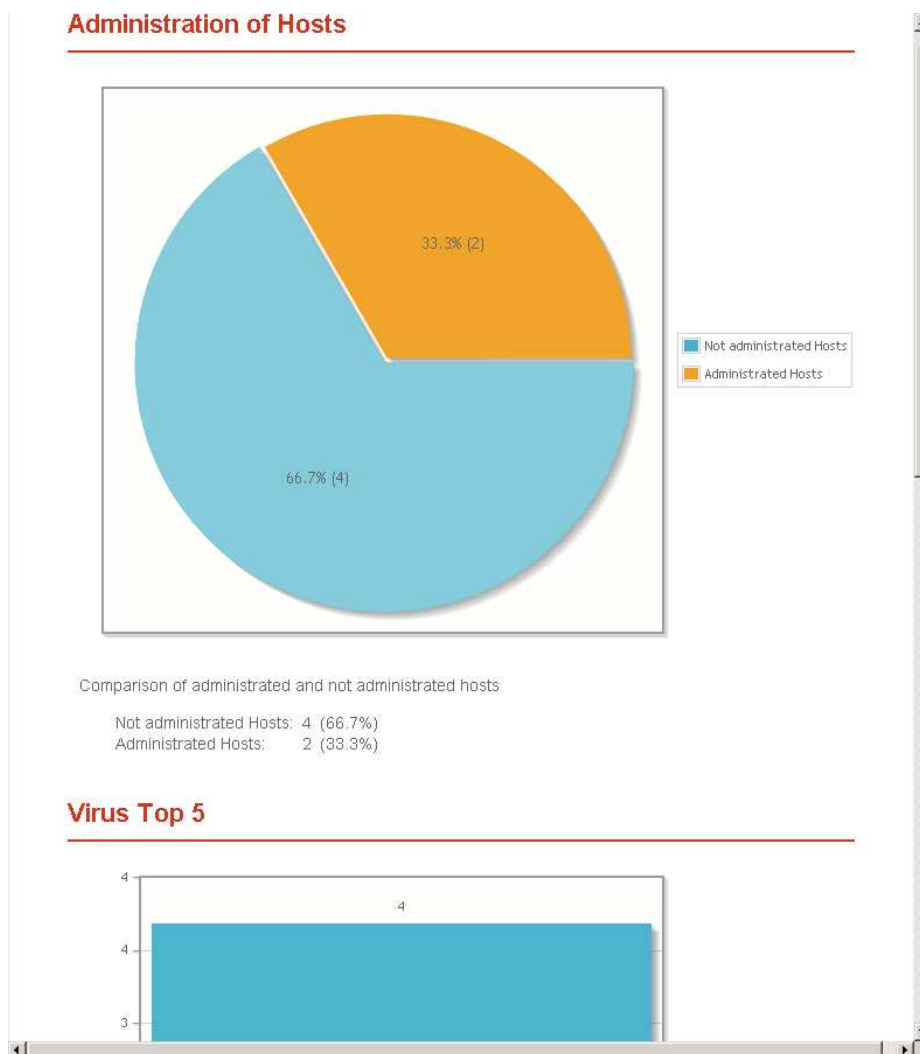


Figure 48: UI – Charts Page

6.3 Footer Window

The footer window is separated in 4 tabs:

- Pending Tasks
- Virus List
- Log File
- Change Log

6.3.1 Pending Tasks

Actions such as installing the IKARUS anti.virus or [\(un\)administering](#) clients are configured as tasks on the IKARUS security.manager Server. Tasks are session-specific and processed tasks get lost when the IKARUS security.manager UI login session is closed. Not finished tasks are still available. The Pending Tasks window (Figure 49) displays all available tasks (either [client](#) specific and for the whole [Directory](#) tree) with their current states, results and resolve times. Consider the resolve time the date when the task state will be re-evaluated. Depending on the task state, an action will be performed to resolve the task.

Keep in mind that next scheduled time may be outdated because automatic refresh is deactivated or the update interval is set higher. Therefore this timestamp is as new as the last refresh occurred!

6.3.1.1 Layout

Toolbar on the top of the window

The elements of the toolbar are described from left to right (see Figure 49):

- Pending:
Shows or hides pending tasks.
- Active:
Shows or hides active tasks.
- Waiting:
Shows or hides waiting tasks.
- Processed:
Shows or hides processed tasks.
- Client specific:
Displays tasks from the currently selected node in the Directory if enabled, otherwise all tasks are displayed.
- Refresh:
Retrieves an updated task list.
- Automatic Refresh:
Retrieves an updated task list automatically based on the user-defined update Interval.
- Update Interval:
Sets the update interval of the task list.

6.3.1.1.1 The Pending Tasks list

In the Pending Tasks List all tasks that are available on the IKARUS security.manager Server are shown, with their current status, since the last update from the server. If a task was restarted, it is shown as sub task in the task list. Those tasks show the status of the tasks, see section 6.3.1.2. Double-clicking a task will open the detail view, see Section 6.3.1.3.

The Next Scheduled Resolve Time shows the date and time when all tasks will be started again and the server will try to resolve them.

6.3.1.1.2 The Context Menu for Pending Tasks

The context menu is opened by a right-click on a task in the pending task list. There are several actions available in the context menu:

- Force:
Forces the completion of the task.
- Stop:
Stops the completion of the task.
- Restart All:
Restarts all subtasks.
- Restart Incomplete:
Restarts only the incomplete subtasks.
- Details:
Opens the detail task view, see Section 6.3.1.3.

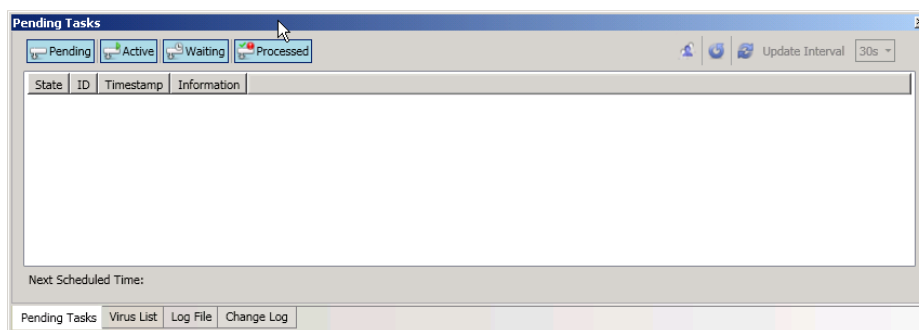


Figure 49: UI – Pending Tasks

6.3.1.2 Task States







Symbol	State	Reason	Action on Resolving
	Active	The action is currently in progress.	Evaluates the task state only.
	Pending	The action has not been processed yet.	The task will be processed soon.
	Waiting	The action has been launched at least once but the target client(s) were not reachable.	Will retry to reach target clients.
	Processed	The action was successfully processed.	Evaluates the task state only.
	Not processed	The action was not processed because the user cancelled the task.	Evaluates the task state only.
	Processed with an error	The action was processed but there was an error during the action.	Evaluates the task state only.

Table 4: Task States - Symbols

6.3.1.3 Task Details

6.3.1.3.1 Toolbar

- Number of Hosts:
Shows the amount of hosts which are targeted in this task.
- Refresh:
Retrieves an updated host- and task-list.
- Automatic Refresh:
Retrieves an updated host list automatically based on the user-defined update interval
- Update Interval:
Sets the update interval of the host list.

6.3.1.3.2 Host List

In the first column the Host State is described, which shows the status of the target host, see Section 6.1.3. The Hostname of the target host is shown in the second column and the Result of the action is shown in the last column.

6.3.1.3.3 Context Menu

On right click on a host list entry the context menu opens, where the following two actions are available:

- Force:
Forces the completion of the task on this host.

- **Cancel:**
Cancels the completion of the task on this host.

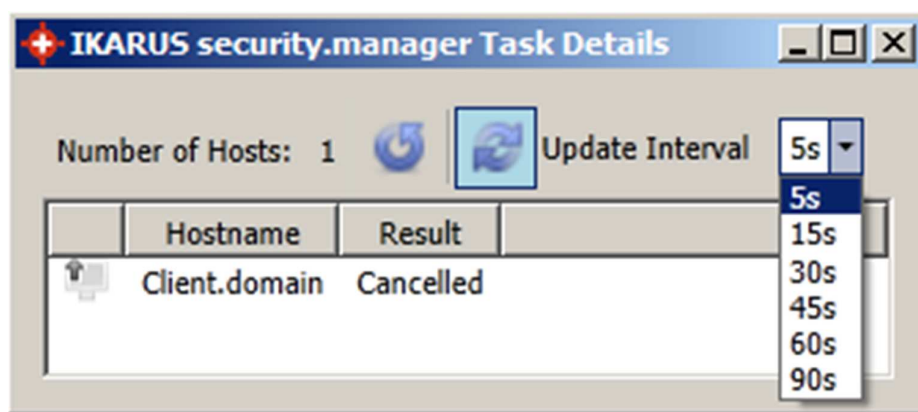


Figure 50: UI – Task Details

6.3.2 Virus List

The Virus List window (Figure 51) is useful for investigating the infections on your network. You can view all infections found or just those on the node currently selected in the [Directory](#).

The buttons „Malware“ and „PUA“ (potentially unwanted application) can be used to hide or show the corresponding types of infections.

6.3.2.1 Layout

On the left side of the information area, in the upper third of the virus list window, you can overall information about the virus list. The information can be minimized through the toggle button “Host specific”. This button shows infections of all clients if enabled, otherwise only those of the currently selected node in the Directory, see Section 6.1.

On the left side of the area the number of viruses shown in the list is outlined.

The virus list consists of several informational columns:

- **Is Active?:**
This column is no longer shown in the virus list (It was only temporarily shown in the 4.0. IKARUS security.manager version). Inactive virus's means that those viruses have been found on hosts that are not administrated by the IKARUS security.manager.
- **Host Status:**
Shows the status of the client, see Section 6.1.3.
- **Hostname:**
Shows the name of the client.
- **Type:**
Shows the type of the infection (either malware or potentially unwanted application)

- **Date:**
The date the infection was found.
- **Filename:**
The filename of the infection.
- **Path:**
The directory the infection was found in.
- **Virus Description:**
The name of the infection. Clicking will open the virus dictionary for this particular infection.

Right click on an infection opens the context menu. In the context menu the following actions can be chosen:

- **Virus Dictionary:**
Opens the virus dictionary entry for the infection.
- **Details:**
Opens the detail view for this infection, see Section 6.3.2.2.
- **Send to IKARUS Virus Lab:**
Sends the infection to IKARUS for analysis.

In case the Host Specific view is active, following options are available too:

- **Temporary Unblock:**
Infected file will be unblocked temporary.
- **Save & Delete:**
Infected file will be deleted from the host.
- **Ignore Virus:**
Virus will be removed from the Virus List, but not from the Host. The next time the host sends its virus list to the IKARUS security.manager, the infection shows up again.

In the action area (it can be found at the bottom of the window) several functionalities are provided that are also available in the IKARUS anti.virus.

- **Select All:**
(De)Selects all entries.
- **Refresh button:**
Refresh the virus list.
- **Purge System:**
Deletes the selected infections of the list.
- **Temporary Unblock:**
Releases the file from quarantine.
- **Save & Delete:**
Creates a backup of the infected file and deletes the original.

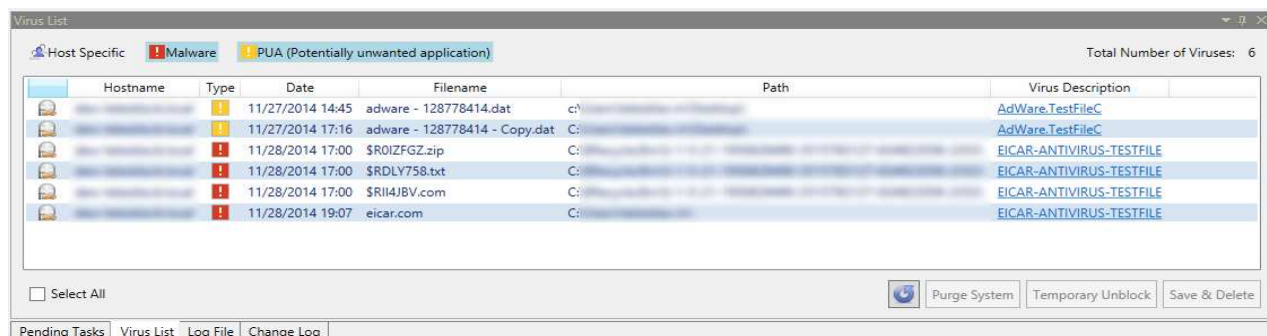


Figure 51: UI – Virus List

6.3.2.2 Virus Information

The Virus Information window displays useful information about a particular infection. You can copy the information to the clipboard by clicking the Copy to Clipboard button.

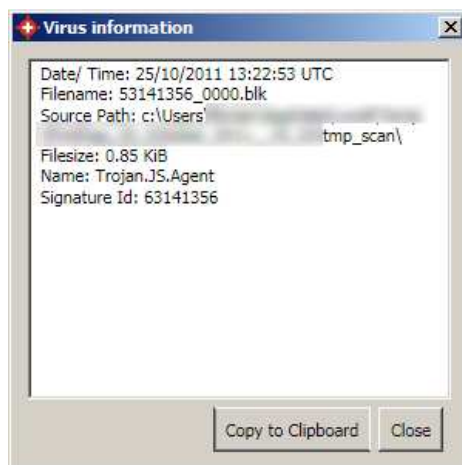


Figure 52: UI – Virus Information

6.3.3 Log File

The Log File window (Figure 53) provides useful information on the background actions performed by the IKARUS security.manager Server. If you encounter unusual behaviour or any kind of problem, the Log File window is an easy way to access the IKARUS security.manager Server log from anywhere using the IKARUS security.manager UI. In addition, you can narrow the information to be displayed: Alerts, Warnings or just information. This simplifies investigating the root cause of a problem. Alternatively, you may use the search field to step through the Log File.

6.3.3.1 Layout

In the upper area of the Log File window it is possible to decide what information is displayed and how often the information is updated from the server.

The buttons described from left to right:

- Alert:
Shows or hides alerts.
- Warn:
Shows or hides warnings.
- Info:
Shows or hides information.
- Refresh:
Retrieves an updated log file from the ISM server.
- Automatic Refresh:
Retrieves an updated log file from the ISM server automatically based on the user-defined update interval.
- Auto Scroll:
Scrolls to the bottom of the log file on automatic refreshes.
- Update Interval:
Set the interval at which the log file should be updated.

Beneath this area the log file is shown. In the log file you can press the right mouse button to open the context menu. In the context menu you can either press “Select All” (to select all the text of the log file) or “copy to clipboard”.

In the lower area it is possible to search for special text in the log file. Just enter the text, you want to search for, in the text box and press the loop to search the log file. The search will start from the position of the text cursor in the log file.

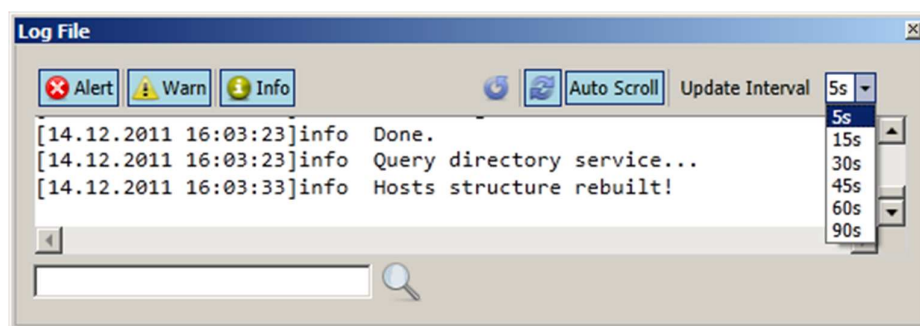


Figure 53: UI – Log File

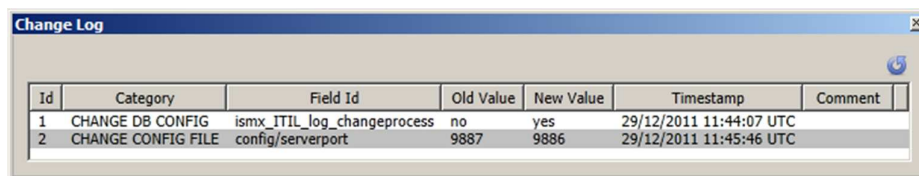
6.3.4 Change Log

The Change Log window (Figure 54) provides an overview of the changes a user made to settings and when they have occurred. Keep in mind that the Change log is only available in single mode.

6.3.4.1 Layout

The change log can be refreshed with the refresh button in the upper right corner and in the list all changes in the IKARUS security.manager can be seen. The columns of the list are:

- Id:
Identification number of the modification.
- Category:
Shows where the modification happened.
- Field Id:
Shows which particular setting was modified.
- Old Value:
Shows the value before the modification.
- New Value:
Shows the value after the modification.
- Timestamp:
Shows when the value modification happened.
- Comment:
Shows the comment entered at the login process.



Id	Category	Field Id	Old Value	New Value	Timestamp	Comment
1	CHANGE DB CONFIG	ismx_ITIL_log_changeprocess	no	yes	29/12/2011 11:44:07 UTC	
2	CHANGE CONFIG FILE	config/serverport	9887	9886	29/12/2011 11:45:46 UTC	

Figure 54: UI – Change Log

6.4 The Menu Bar

The menu bar is located at the top of the IKARUS security.manager UI main window.

The menu bar includes the following sub-menus:

- File Menu (Figure 55)
- View Menu Figure 56)
- Tools Menu (Figure 57)
- Help Menu (Figure 67).

6.4.1 File Menu

The File Menu includes the following entries:

- Update ISM (F6):
Invokes an update process of the ISM server.
- Exit (Alt+F4):
Quits the current session and the ISM UI.
- Logout (Ctrl+Alt+F4):
Quits the current session and opens the Login window.

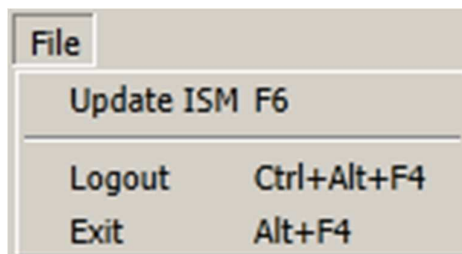


Figure 55: UI – Menu Bar – File Menu

6.4.2 View Menu

The View Menu includes the following entries:

- Overview Page:
Shows or hides the Overview Page, see section 6.2.2.
- Directory:
Shows or hides the Directory, see section 6.1.
- General:
Shows or hides the General Page, see section 6.2.3.1/6.2.3.2.
- Properties:
Shows or hides the Properties Page, see section 6.2.4.
- Pending Tasks:
Shows or hides the Pending Tasks window, see section 6.3.1.
- Virus List:
Shows or hides the Virus List, see section 6.3.2.
- Log File:
Shows or hides the Log File, see section 6.3.3.
- Change Log:
Shows or hides the Change Log, see section 6.3.4.
- Restore Default Layout:
Restores the default window layout.
- Toolbars/Main toolbar:
Shows or hides the Main toolbar, see section 6.5.

- IKARUS anti.virus Configurations:
Opens the IKARUS anti.virus Configurations Window, see section 6.5.1.

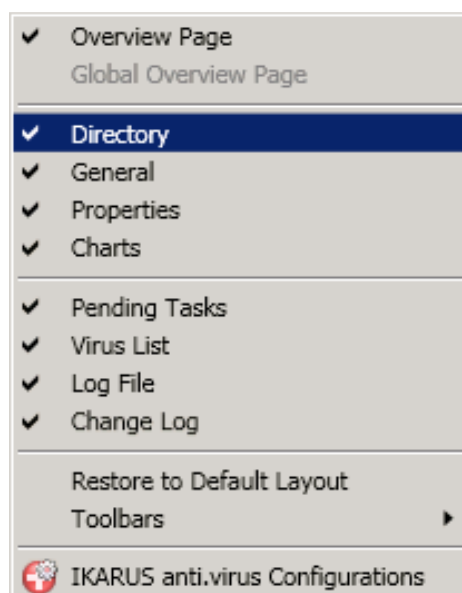


Figure 56: UI – Menu Bar – View Menu

6.4.3 Tools Menu

The Tools Menu includes the following entries:

- Options (F12):
Opens the IKARUS security.manager Options window, see section 6.4.3.2.
- Clean host-entries from database:
It is possible to clean up the database from unused hosts by using the dialog “Clean host-entries from database”. For further information on this dialog see section 6.4.3.1.
- Change Password:
Opens the Change Password window where you can set a new password for the IKARUS security.manager.
- Change Language:
Opens the Change Language window where you can select a different IKARUS security.manager UI language. Changing the UI language does not require a program restart.
- IKARUS Virus Dictionary:
Opens the default web browser and changes to the IKARUS Virus Dictionary.
- Save Support Info:
Generates a “[ZIP](#)” file that is provided by the IKARUS security.manager Server that can be saved on your local system. This file holds all necessary information which the support department of IKARUS Security Software needs to retrieve information about your system. Additionally a database backup file is also created. Please keep in mind that the database user has to have also write rights on the IKARUS security.manager shared directory and the host, where the

database is running, should be able to access the shared directory. Otherwise there is no possibility to copy automatically the file from database host (if this is another one than the host where IKARUS security.manager is running).

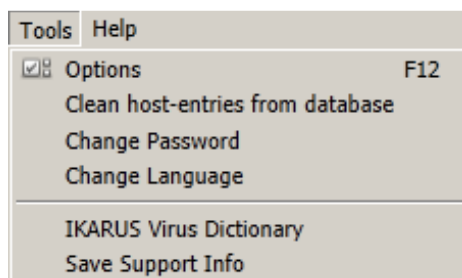


Figure 57: UI – Menu Bar – Tools Menu

6.4.3.1 Dialog “Clean host-entries from database”

This dialog should only be used if hosts were manually deleted from the Active Directory. In this case the deleted hosts may still be available in the database, and this dialog provides a way to finally delete them from the database. Please note that the selected hosts will be deleted irrevocably!

On the left side of the dialog all unused hosts are displayed. These are hosts that are still in the database and managed, but do no longer appear in your [Active Directory](#) or in your manual group. This can occur, because the IKARUS security.manager does not automatically deletes hosts from the server when they are no longer available in the [Active Directory](#), because the server cannot assume the user behaviour.

An administrator of the IKARUS security.manager must manually remove those hosts, by moving a host from the left list, “Deleted hosts from Active Directory”, to the right list, “Hosts that will be deleted”. To move a host from one list to the other, there are 4 buttons in the middle of the two lists:

- Select all hosts:
All hosts are set to remove host list
- Select one host:
Selected host is set to remove host list
- Unselect one host:
Selected host is deleted from remove host list
- Unselect all hosts:
All hosts are deleted from remove host list

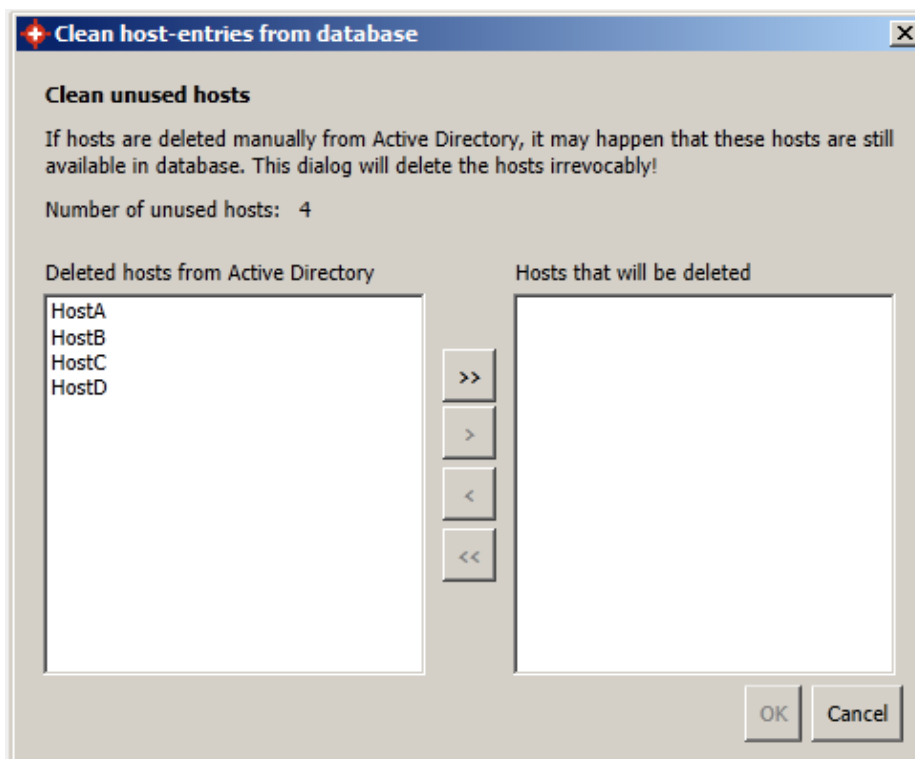


Figure 58: UI – Clean host-entries from database

Cleaning up the database from unused hosts, licenses that were assigned to the selected hosts may be given free. This dialog is available under Tools → Clean host-entries from database.

6.4.3.2 Dialog “Options”

The IKARUS security.manager Settings window shows settings for the IKARUS security.manager Server (see Figure 59). The window is separated into five tabs: General, E-Mail Notifications, Update, Fileshare, LDAP and Charts. Changes to the settings are committed upon clicking the OK or Apply buttons at the bottom of the window. These two buttons will be disabled when entries are missing or invalid. Clicking the Cancel button will close the window and discard all changes, clicking the OK button will save all changes and close the window.

6.4.3.2.1 General

In the General tab the following settings can be set:

- **Shared Directory:**
Sets the directory where ismxstartup.exe is stored for the IKARUS anti.virus deployment.
Open Browser Button:
Opens a browser window for choosing the shared directory.
Keep in mind that appropriate read and write rights should be set (see chapter 7)

- **Enforce Client Update:**
Enable or disable deployment over TCP.
- **Enforce Client Update Port:**
Enable deployment over specified TCP port.
- **Administration Port:**
The port the IKARUS security.manager UI uses for communicating with the IKARUS security.manager Server.
- **Automatically Add Clients:**
Specifies whether new clients in the LDAP are automatically added to the Directory.

The **Performance Settings** can be used to improve **IKARUS security.manager** performance:

- **Maximum Number of Simultaneous connections:** Defines how many simultaneous connections the IKARUS security.manager accepts. This affects connections between IKARUS security.manager GUI and server as well as connections to IKARUS anti.virus installations. This setting has no influence on the number of managed hosts. 0 for infinite simultaneous connections.
- **Maximum Number of Simultaneous Downloads:** In case no fileshares are available, managed IKARUS anti.virus installations load updates directly from the IKARUS security.manager server. This setting defines how many hosts can update at the very same time. 0 for infinite simultaneous downloads

In the Change Management section the following settings can be enabled or disabled:

- **Enable Change Management according to the ITIL:**
Enables or disables change tracking.
- **Ask for comment at Log-in screen:**
If enabled, the user must enter a comment on login attempts.
- **Maintain change log for server settings:**
If enabled, logs all changes made to settings.
- **Ask for Request for Change (RfC) ID:**
If enabled, the user must enter an RfC ID on login attempts.

In the “Used config after drag and drop” section the following settings can be done:

- **Drag and Drop Behaviour:**
If enabled, user gets a notification what to do with config files after moving hosts in manual group.
- **Define Standard Behaviour:**
If the same behaviour should be applied in every case, then choose if hosts should use own or parent config file.

Signature Quality Assurance is an **IKARUS anti.virus** functionality to send anonymous information about infections to IKARUS for better analysis. Is SigQA enabled, all managed hosts participate.

Debug Logging activates extended, server-side logging. This can be helpful in support cases

The screenshot displays the 'General' tab of the IKARUS security.manager settings. At the top, there are tabs for 'General', 'E-mail Notifications', 'Update', 'Fileshare', 'LDAP', and 'Charts'. The 'General' tab is active, showing a text field for 'Shared directory for remote installation:' with a browse button (...). Below this are several settings: a checked checkbox for 'Enforce Host Update' with a port of '9888', an 'Administration Port' of '9887', and a dropdown for 'Automatically Add Hosts' set to 'Yes'. A 'Performance Settings' section contains 'Maximum Number of Simultaneous Connections' (0) and 'Maximal Number of Simultaneous Downloads' (10). The 'Change Management' section has four unchecked checkboxes: 'Enable Change Management according to the IT Infrastructure Library (ITIL)', 'Ask for comment at Login screen.', 'Maintain change log for server settings.', and 'Ask for Request for Change ID (RfC)'. The 'Used config after drag and drop:' section has a checked checkbox 'Inform user about different configs after drag and drop' and two radio buttons: 'own config' (selected) and 'parent config'. The 'Signature Quality Assurance (SigQA)' section has a checked checkbox 'Enable SigQA for all hosts'. The 'Debug Logging' section has a checked checkbox 'Enable Debug Logging'. At the bottom right are 'OK', 'Cancel', and 'Apply' buttons.

Figure 59: UI – IKARUS security.manager Settings – General

6.4.3.2.2 E-Mail Notifications

In the e-mail tab the following settings can be set:

- Enable e-mail Reports:
Enable or disable e-mail reports.

- Mail Server:
Defined mail server over that the reports are sent.
- Sender:
The address from which the reports are sent.
- Enable Authentication:
Enables or disables user authentication with the e-mail server.
- Username:
The username used to authenticate with the e-mail server.
- Password:
The password used to authenticate with the e-mail server.
- Available Reports:
Lists all available reports.
- Add New Report:
Open the IKARUS security.manager Reports window, see Section 0.

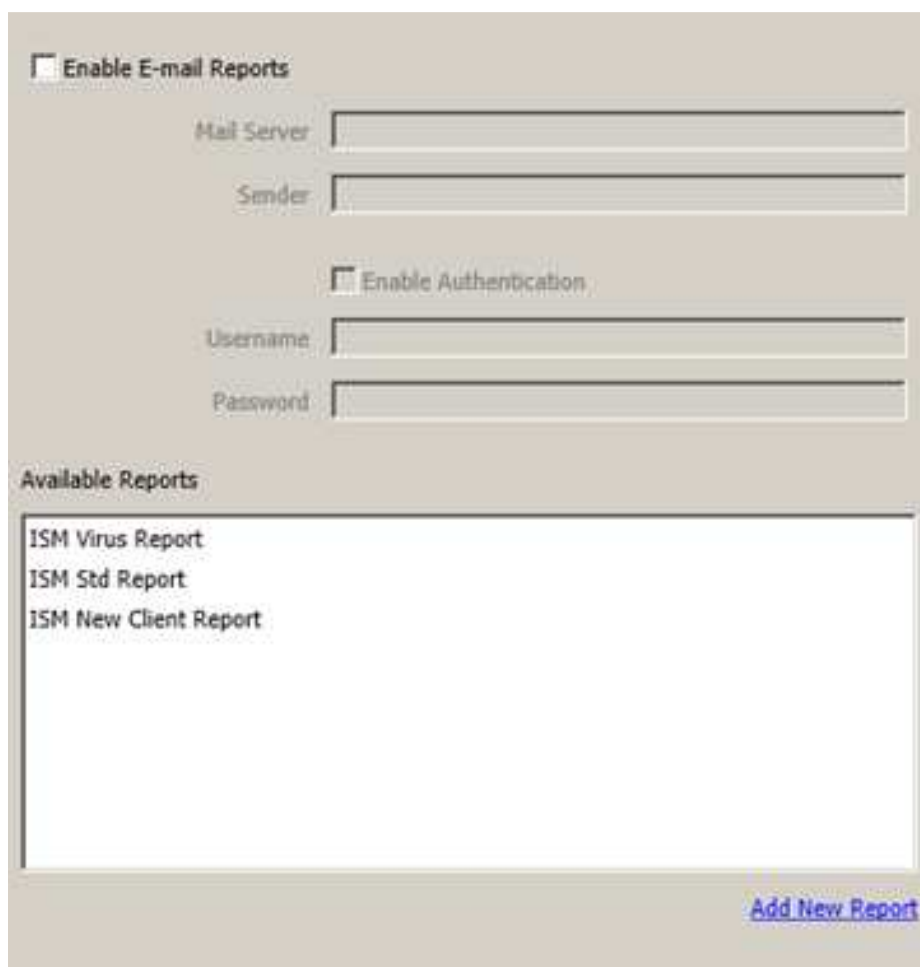
The image shows a screenshot of the "IKARUS security.manager Settings – E-Mail Notifications" window. At the top, there is a checkbox labeled "Enable E-mail Reports". Below this, there are two text input fields: "Mail Server" and "Sender". Further down, there is another checkbox labeled "Enable Authentication". Below this, there are two more text input fields: "Username" and "Password". At the bottom of the window, there is a section titled "Available Reports" which contains a list of three reports: "ISM Virus Report", "ISM Std Report", and "ISM New Client Report". In the bottom right corner of the window, there is a blue button labeled "Add New Report".

Figure 60: UI – IKARUS security.manager Settings – E-Mail Notifications

IKARUS security.manager Reports

In the reports dialog the following settings can be set to configure the e-Mail report:

- Report Name:
Sets the name of the report.
- Enable Report:
Enables or disables sending of this report.
- Report Type:
Sets the type of the report. Following types are available:
 - ✓ "On Virus" Report:
Send report when a virus is found.
 - ✓ "On Auto-Add" Report:
Send report when a computer is added to the LDAP automatically.
 - ✓ Day Report:
Send report on the set days.
 - ✓ ISM Server Startup Report:
Send report as the server starts up.
 - ✓ Interval Report:
Send report at the specified time.
 - ✓ License expires Report:
Send report some days before the license is about to expire.
- Scheduled Time:
Sets the time when the report is sent.
- Day Mask:
Sets the days on which the report is sent.
 - ✓ Enable Virus Report:
Include virus information.
 - ✓ Enable Version Report:
Include version information.
 - ✓ Enable Client Report:
Include client information.
 - ✓ Enable Server Report:
Include server information.
- Add Button:
Add a recipient for the report.
- Recipients:
List of all recipients of the report.

IKARUS security.manager Reports

Report Name: ☒ Enable Report

Report Type:

Scheduled Time: :

Day Mask: ☒ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday
☐ Friday ☐ Saturday ☐ Sunday

Reports: ☒ Enable Virus Report
☐ Enable Version Report
☐ Enable Client Report
☐ Enable Server Report

Add new Recipient:

Recipients:

Figure 61: UI – IKARUS security.manager Settings – Reports

Virus Report:

The virus report can either be set as a separate report type, which then will be sent, when a new virus is found in your system, or as report information additional to a different report, e.g. day report. The report has the following format:

```
-----  
-  
ISM Virus Report:  
testuser1.ikarus.at is infected with 1 virus(es)  
testuser2.ikarus.at is infected with 38812 virus(es)  
  
testuser1.ikarus.at:  
c:\Users\TestUser1\Desktop\eicar.com (EICAR-ANTIVIRUS-TESTFILE)  
  
testuser2.ikarus.at:  
Detailed virus data for this host is currently not available on ISM!  
-----  
-
```

It might happen that not all virus information is available for a host on the ism side (e.g.: Host was turned off after infection detection by user and the IKARUS anti.virus was not able to upload all information to the IKARUS security.manager Server). When this occurs the report only holds the information “Detailed virus data for this host is currently not available on ISM!”. You can either connect to the IKARUS security.manager Server and check when the data is available in the virus list (see section 6.3.2) or you can start IKARUS anti.virus in the IKARUS security.manager UI (see section 6.1), where the viruses were found.

6.4.3.2.3 Update

In the Update tab the following settings can be set:

- Silent Update of the IKARUS security.manager Server:
Enables the automatic update of the IKARUS security.manager Server.
- Proxy Server:
Sets the proxy server through which the IKARUS security.manager Server is accessing the updates.
- Proxy Port:
Sets the port the connection is established through.
- Username:
Sets the username for authenticating with the proxy server if needed.
- Password:
Sets the password for authenticating with the proxy server if needed.

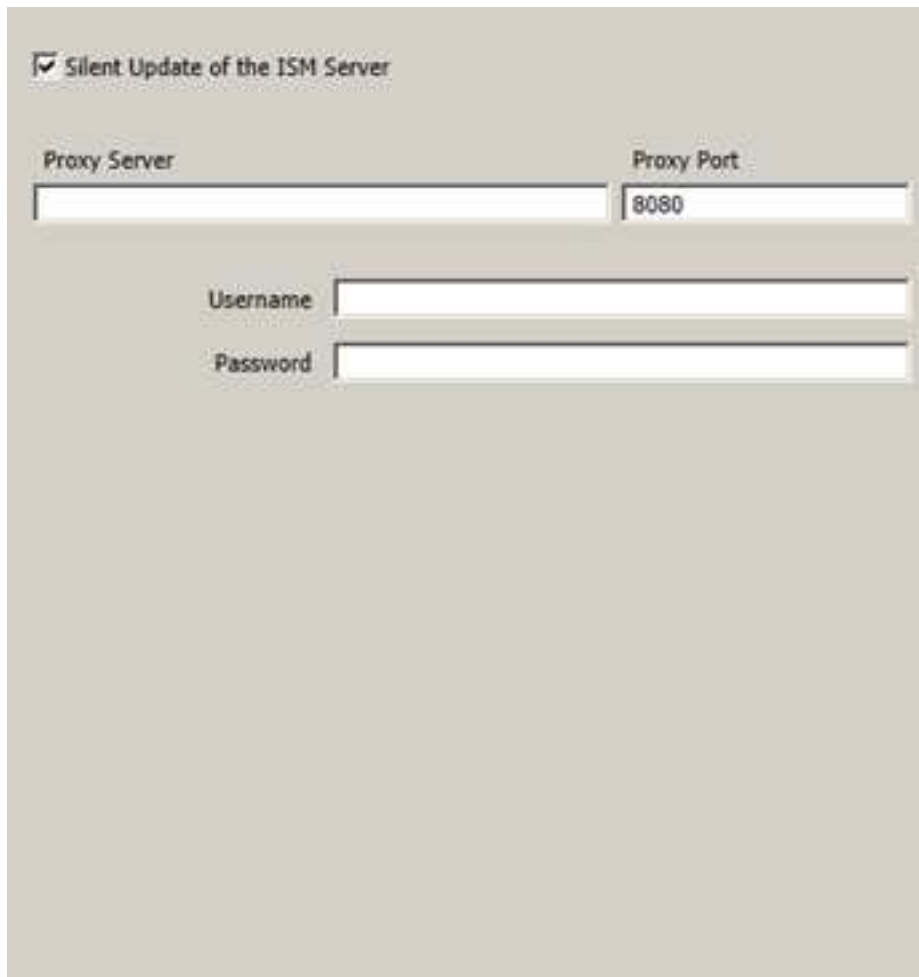


Figure 62: UI – IKARUS security.manager Settings – Update

6.4.3.2.4 Fileshare

For avoiding resource bottlenecks, [fileshares](#) should be used. Administrators have to first create [fileshares](#) for the usage with IKARUS security.manager. Please notice, that the IKARUS security.manager Server needs read and write rights for keeping data up to date. Figure 63 shows the [fileshare](#)-tab.

In the fileshare tab the following information in the list can be seen:

- Online/Offline:
A fileshare is set to online if all files are available and up to date.
- Randomized Pool:
If a fileshare is in the randomized pool then it will be randomly assigned to a host that actually needs an update.
- Fileshare List:
Contains all active or inactive fileshares

The following two actions can be performed in the fileshare tab:

- Start Rollout:
If new fileshares are added, users may want to start immediately a rollout of the files.
- Add fileshare:
Adds a new fileshare. Fileshares will be set to online as soon as all files are copied by the rollout process

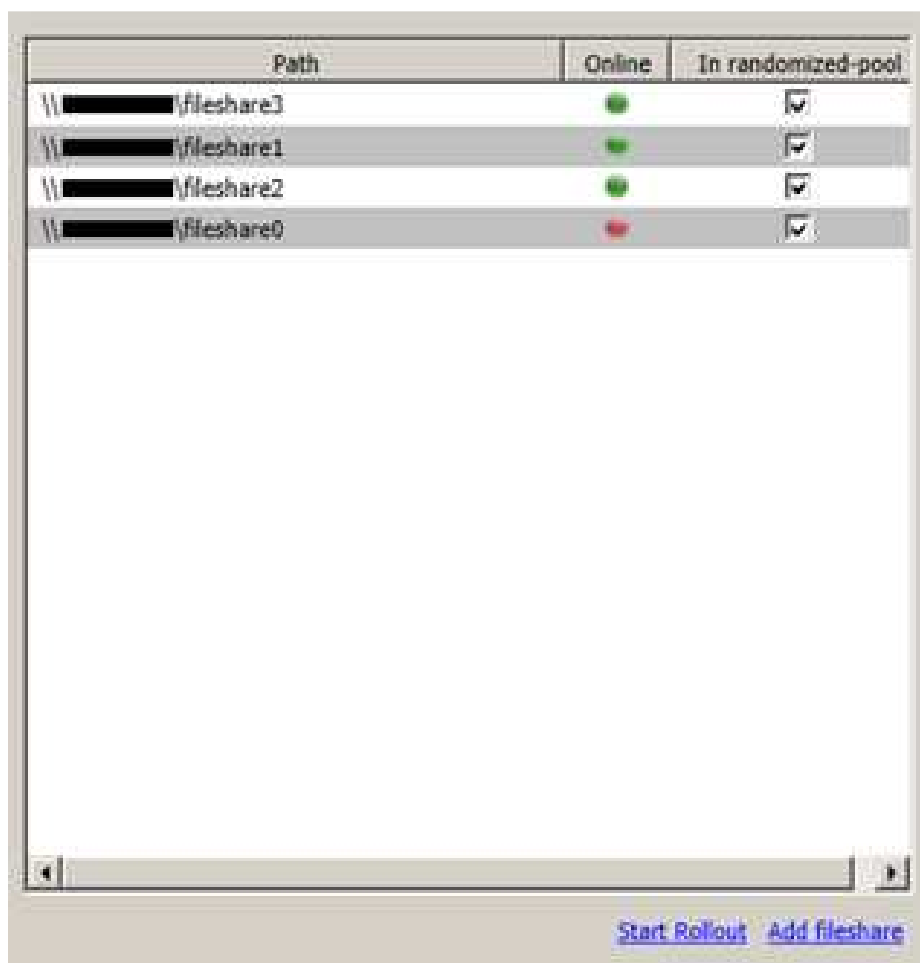


Figure 63: UI – IKARUS security.manager Settings – Fileshare

The IKARUS security.manager Server checks every minute if a [fileshare](#) is available or not. The actual state is visualized by ● ([fileshare](#) is online) or ● ([fileshare](#) is offline), see Figure 63 second column. A [fileshare](#) is available if all necessary files are existing and up to date.

Furthermore IKARUS security.manager Server checks every 20 minutes if updates are available and need to be copied to the defined [fileshares](#). It is also possible to start the rollout-process of the update-files manually with “Start Rollout” (see Figure 63).

A clean-up process, which is triggered once per day, deletes old files for keeping the amount of data as small as possible.

A [fileshare](#) is set to a corresponding host or group by the help of the properties page in section update (see section 6.2.2).

6.4.3.2.5 LDAP

In the [LDAP](#) tab the user can configure the [LDAP](#) settings by changing the following settings:

- Auto Detect Domain:
Try to auto detect the domain
- Server name:
Name of domain controller (see section 9.2)
- Type:
Type of [LDAP](#) (see section 9.2)
- Attribute:
Sets attribute to read (see section 9.2)
- Search path:
Defines domain for scanning (see section 9.2)
- Filter:
Sets the criteria used on resolving the specified attribute (see section 9.2)
- Authentication Method:
Method for authentication on domain controller (see section 9.2)
- Username:
Sets the username for the [LDAP](#) connection (see section 9.2)
- Password:
Sets the password for the [LDAP](#) connection (see section 9.2)
- Exclusions:
Overview of defined exclusions
- Add Exclusions:
Add a new host that will be not listed in directory
- LDAP-Settings Test:
Test if a [LDAP](#) can be found with the given parameters

The Ldap settings can be configured here. It may take a view minutes to update the GUI.

☐ Auto Detect Domain

Servername

Type

Attribute

Searchpath

Filter

Auth Method

Username

Password

Ldap settings not tested.

Exclusions

[Add Exclusion](#)

Figure 64: UI – IKARUS security.manager Settings – LDAP

By the help of the dialog, which is shown in Figure 64, a [LDAP](#) can be used. Previously a [LDAP](#) was configured in the config-file. If a <ldap> section is within the config file, then this section is read and set by the IKARUS security.manager Server automatically. Afterwards the <ldap> section will be deleted from the config file.

Therefore two ways are possible for setting a [LDAP](#):

- Use the [LDAP](#)-tab within the IKARUS security.manager Settings
- Add the <ldap> section to the config file

More information about the config file and [LDAP](#) parameters may be found in chapter 9 as well as in section 9.2.

6.4.3.2.6 Charts

In the Charts tab it is possible to modify the appearance of the standard charts and change description text (see Figure 65).

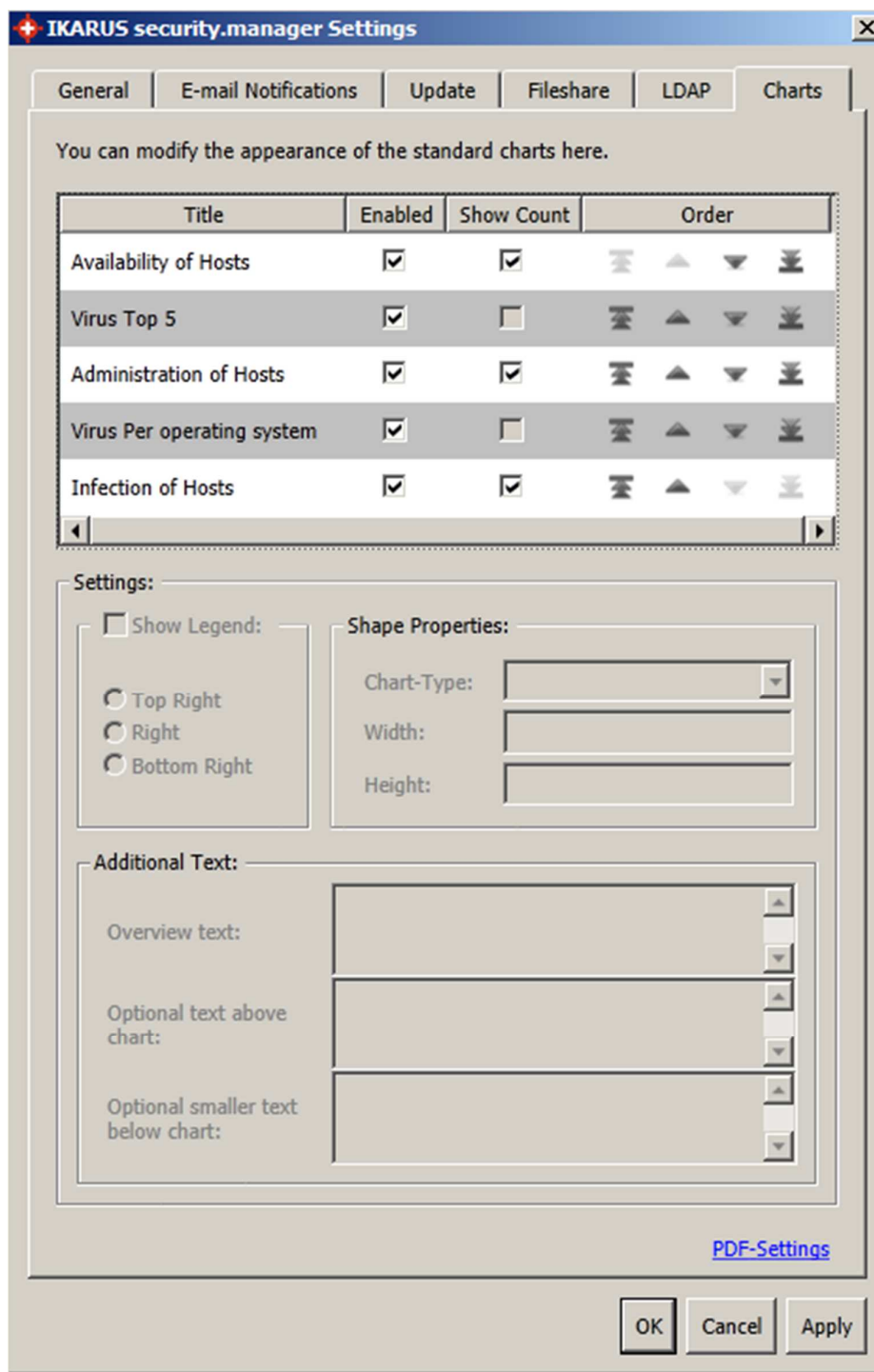


Figure 65: Charts options

In the upper section of dialog the 5 standard charts are listed.

- With the arrow keys it is possible to change the order of the charts.

- Through the enabled checkbox it is possible to hide charts from the Charts Page as well as in the PDF (see section 6.2.5).
- If the chart type is “pie-chart”, it is possible to show the count next to the percentage in the pie chart by checking the “Show-Count” checkbox.

The settings are divided into 3 parts. Those settings depend on the chart that is selected in the charts list above.

In the “Show Legend” part it is possible to decide where the legend of the chart is situated (Top Right, Right, Bottom Right) and if a legend is even displayed.

In the “Shape Properties” part the chart type (pie or bar chart) can be chosen and the width and height can be set for any chart, so that it best fits your screen resolution. The minimum width and height for the charts is 500 pixels.

In the “Additional Text” part it is possible to add your customized descriptions. Those descriptions will be displayed in the report and on the Charts Page.

The link “PDF-Settings” in the lower left corner opens a dialog, where you can change the standard header and footer of the report to your personalized header and footer (see Figure 66). It is also possible to revert it to the default header and footer. The footer and header can also be disabled, so that they are not shown in the report. Those settings only affect the appearance of PDF report.

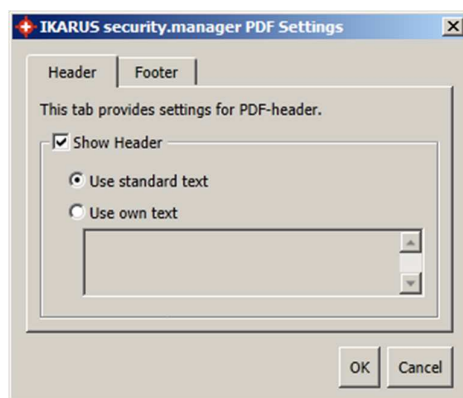


Figure 66: PDF Report settings

6.4.4 Help Menu

The Help Menu includes the following entries:

- User Manual (F1):
Opens this IKARUS security.manager User Manual.

- **Contact Information:**
Opens the Contact Information window.
- **General Business Terms:**
Opens the General Business Terms of the IKARUS security.manager.
- **About IKARUS security.manager:**
Opens the “About” dialog that displays the IKARUS security.manager version and information about the license in use.

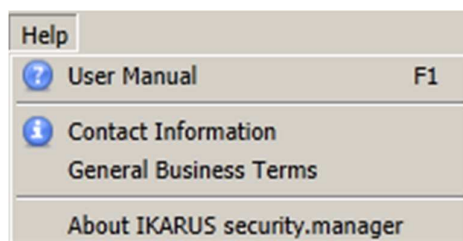


Figure 67: UI – Menu Bar – Help Menu

6.4.4.1 About Dialog

In the About Dialog the information is separated into two sections:

- **Version Information:**
Displays the IKARUS security.manager UI, IKARUS security.manager Server and Updater versions.
- **License Information:**
Displays the expiration date and how much of your license capacity is used and free.

At the bottom of the dialog a user can renew his license by clicking the Renew License link (see Figure 68).



Figure 68: UI – About Dialog

6.4.5 Management Menu

The management menu includes the following entries and is only available when management-mode is activated:

- Options:
Opens the options-window for editing settings of the used IKARUS security.manager-Servers (see section 6.4.5.1).
- Export config:
Using this menu it is possible to export already entered IKARUS security.manager-Server (see section 6.4.5.2).
- Change password for management mode:
Use this dialog if changing the management-mode password is necessary (see chapter 6.4.5.3).
Note, that changes of the management-password have no impact of the password of all entered IKARUS security.manager-Server.

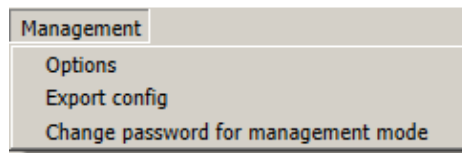


Figure 69: UI – Menu Bar – Management Menu

Via this menu option, you are given access to all the options that concern the management mode of the IKARUS security.manager. Here you are given an overview of your IKARUS security.manager instances and can add, edit or delete them. Furthermore, you can use this menu to export the settings of your

IKARUS security.manager instances to a password protected file, and change the password for the configuration file of management mode.

Please note that this menu is not available in single mode.

6.4.5.1 The "Options" menu

The options dialogue can be found in the main menu under "Options".



Figure 70: UI - "Management" menu, "Export configuration file" menu option

The dialogue provides an overview of your IKARUS security.manager instances. They are shown in the list with the server name, port, username and description. In addition, you can see whether an instance has valid connection data and whether it is setup as the default instance.

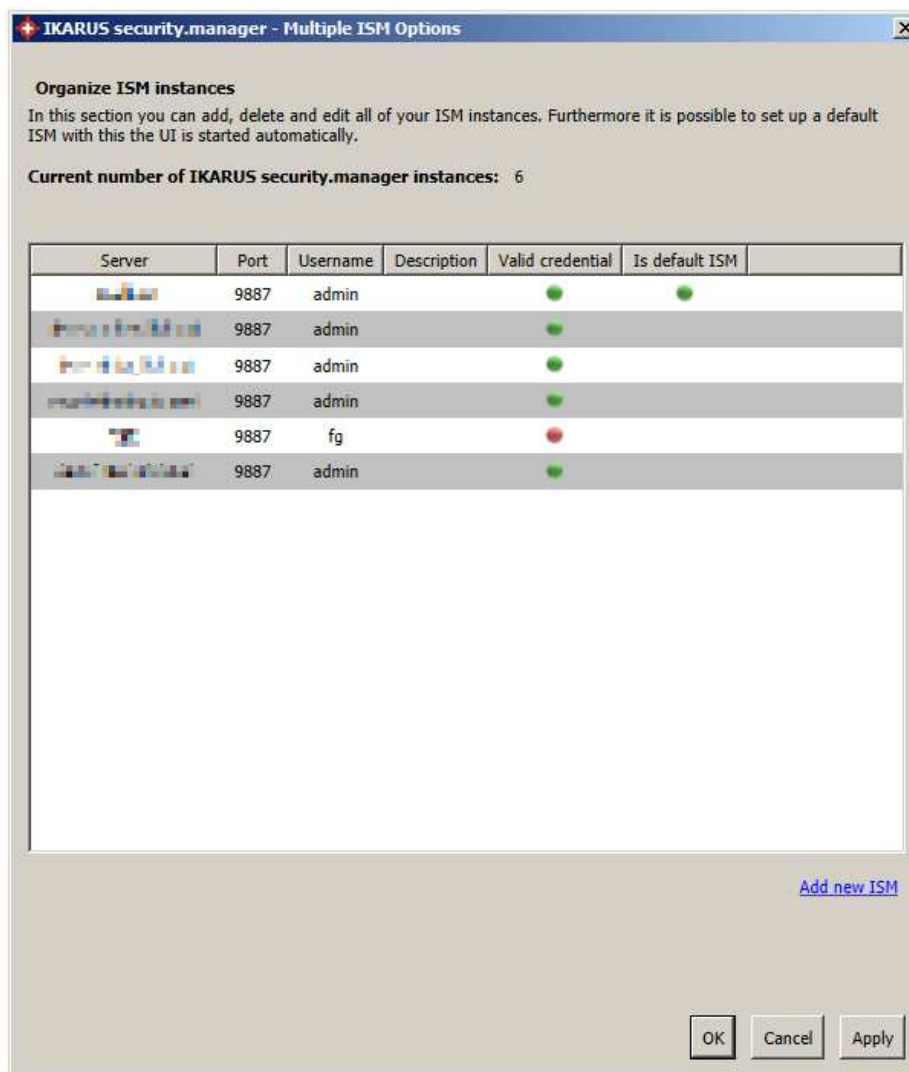


Figure 71: UI – Options dialogue

You can edit and delete the existing instances, and set them to be the default instance. All operations can be called from the shortcut menu.

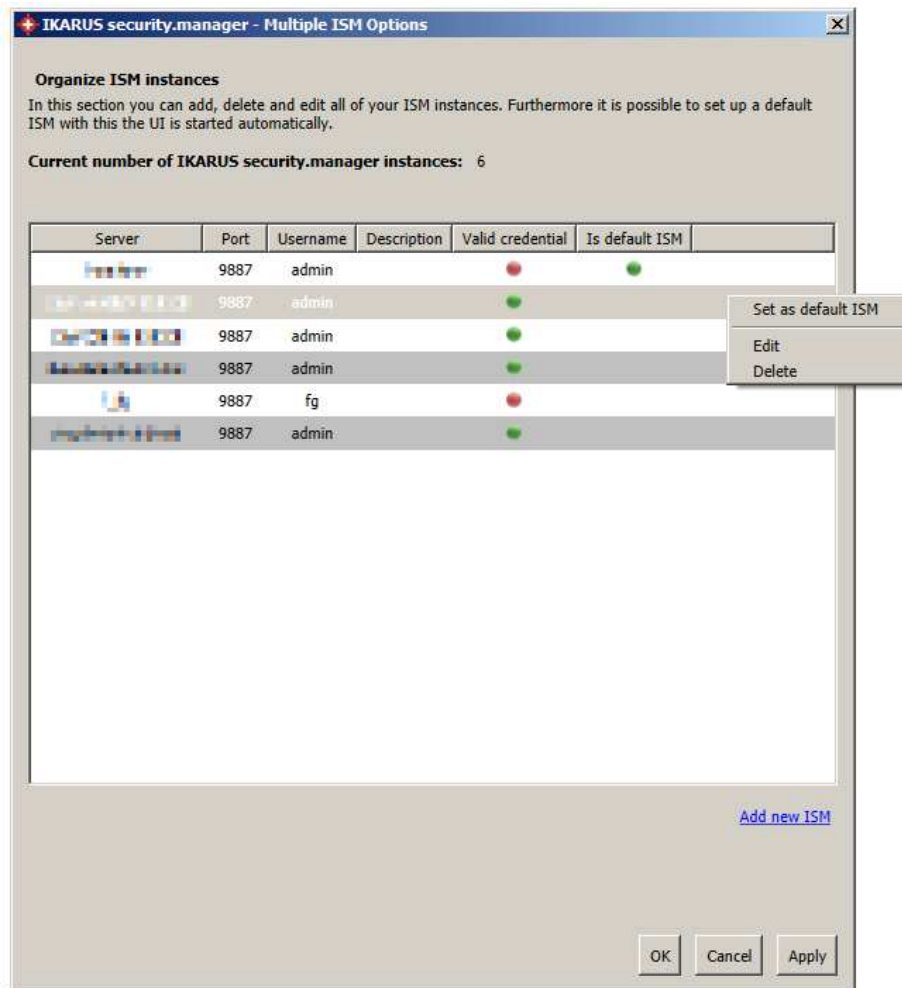


Figure 72: UI – Shortcut menu in the options dialogue

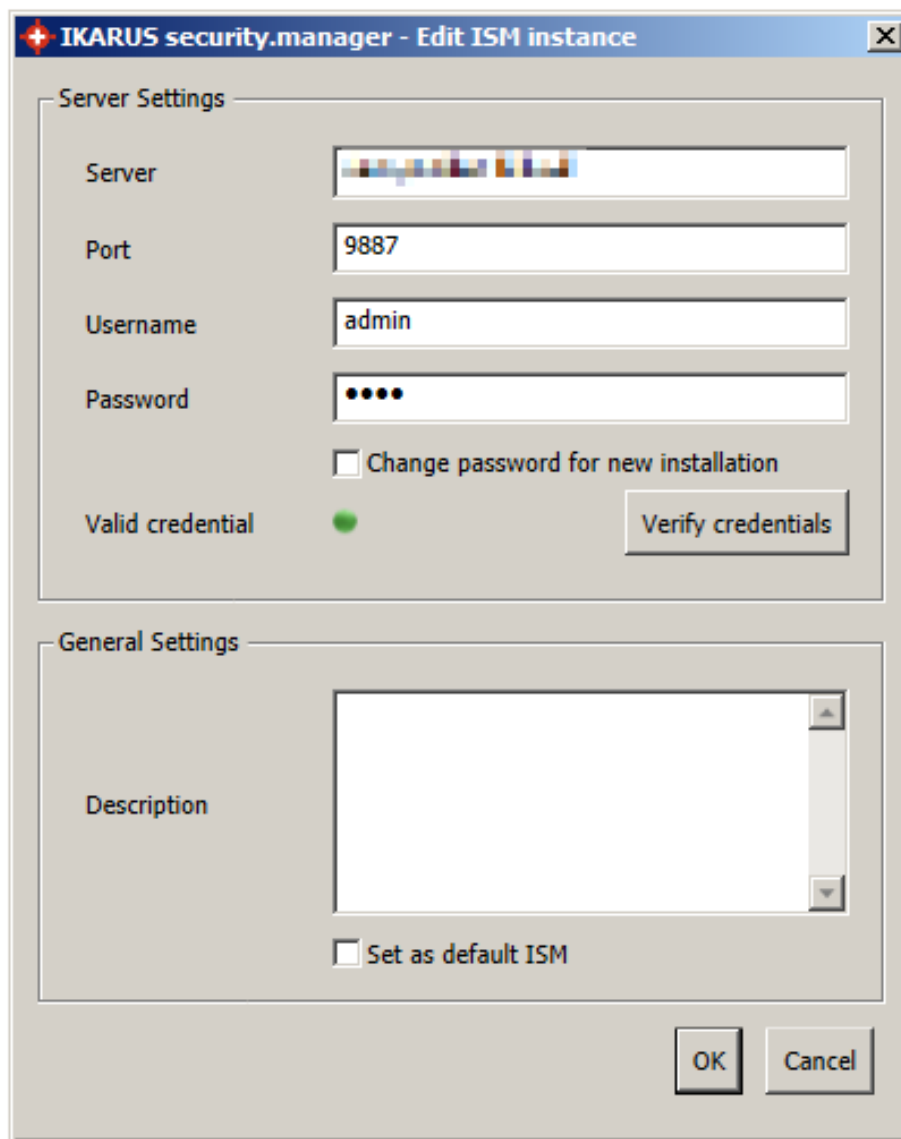
"Set as default ISM" means that when the program restarts, the connection will be established automatically to that IKARUS security.manager instance. There must always be a default instance. You cannot delete it.

If you click "Delete", the selected instance will be deleted from the list. Please note that you cannot delete the IKARUS security.manager instance to which you are currently connected nor the default instance. It is also possible to delete instances by selecting an instance and then pressing the delete key of your keyboard.

6.4.5.1.1 Editing the IKARUS security.manager server

If you click "Edit" in the shortcut menu of an IKARUS security.manager instance, you will reach the edit dialogue. There, you have the possibility to change the server name, port, username, password and description.

As an alternative, you can double-click an IKARUS security.manager instance in the list, which will also open the edit dialogue.



The dialog box is titled "IKARUS security.manager - Edit ISM instance". It is divided into two main sections: "Server Settings" and "General Settings".

Server Settings:

- Server:** A text field containing a placeholder or masked text.
- Port:** A text field containing the value "9887".
- Username:** A text field containing the value "admin".
- Password:** A text field with masked characters (dots).
- ☐ **Change password for new installation**
- Valid credential:** A green dot indicator.
- Verify credentials:** A button.

General Settings:

- Description:** A large text area for entering a description.
- ☐ **Set as default ISM**

At the bottom right, there are **OK** and **Cancel** buttons.

Figure 73: UI - Edit dialogue

The program will make you aware of any invalid input. It is only possible to confirm the data if all entries have been acknowledged as valid. The port number must, for example, lie in a specific range of numbers to be able to successfully create this instance.

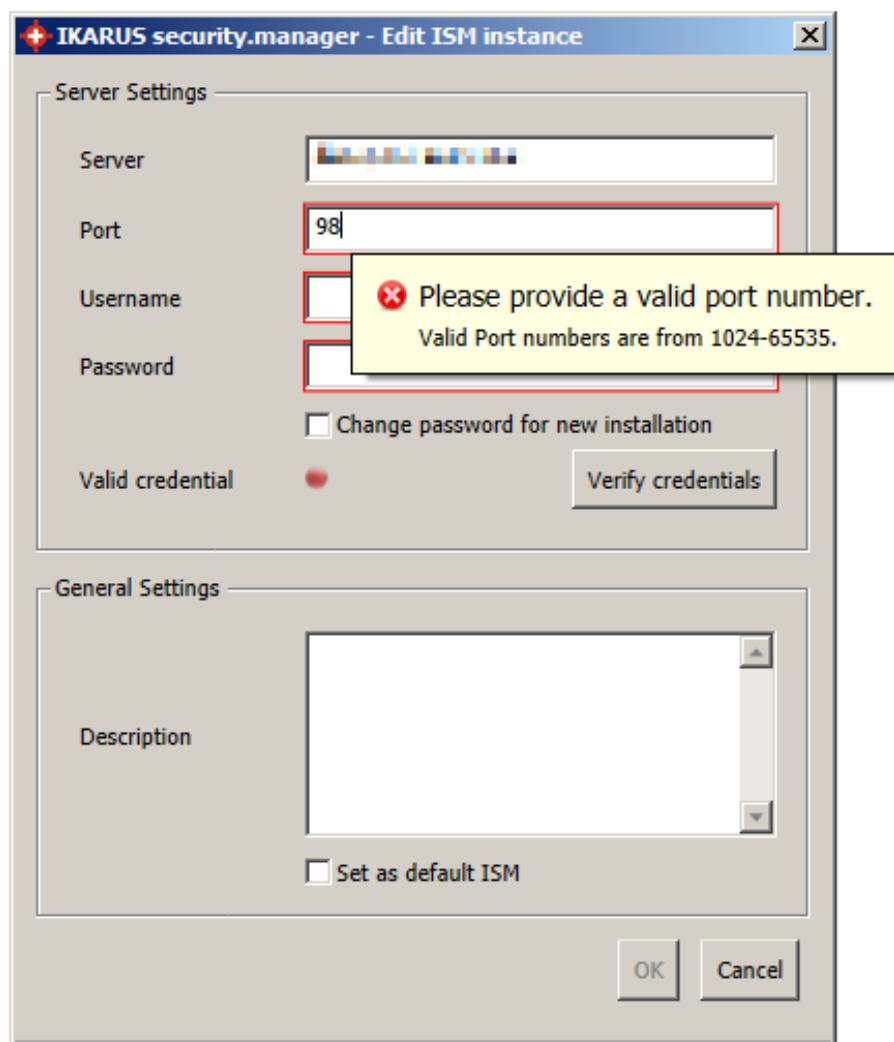


Figure 74: UI - Edit dialogue, entering invalid data

Activate the "Change password for a new installation" option. Then you can change the password of the IKARUS security.manager instance. However, that is only possible after a new installation.

IKARUS security.manager - Add new ISM instance

Server Settings

Server: localhost

Port: 9887

Username: admin

Password: •••••

☐ Change password for a new installation

Valid credentials: ● Verify credentials

General settings

Description:

☐ Set to default ISM.

OK Cancel

Figure 75: UI - Edit dialogue, changing the password for a new installation

You must enter the same value in both password fields. Click "Set password" to check whether the password change is possible. If it is, then the password of the IKARUS security.manager instance will be reset.

Click the "Check connection data" button to have the program check the correctness of the entered data. You will be informed of the result of the verification by a message window as well as the status indicator to the left of the button. It is green if the connection was established successfully, or red if the test connection failed.

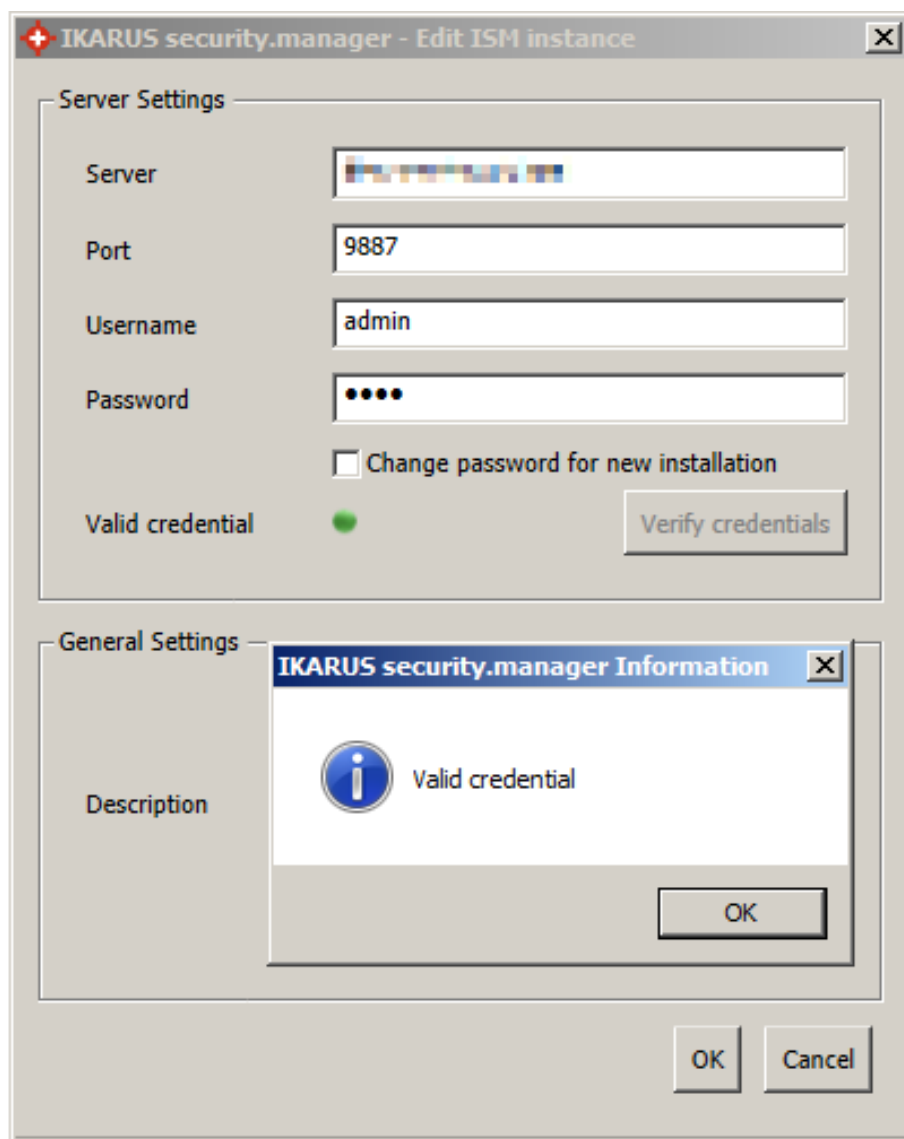


Figure 76: UI - Edit dialogue, checking the access data

With the checkbox on the bottom edge of the dialogue, you define whether the instance is your default instance. You will be automatically connected to the default instance every time the program restarts. Please note that there must always be such a default instance. You may be requested by the program to set this option.

When you have completed all the necessary fields and the entered data is valid, then you can close the edit dialogue by clicking "OK".

6.4.5.1.2 Add IKARUS security.manager server

In addition, it is possible to add new instances in the options dialogue. You can do this by using the "Add instance" link under the list. One click on it opens the edit dialogue described in the previous pages. Naturally, no fields are filled in. You must first of all specify all the required information.

Please note that changes to IKARUS security.manager instances will only be accepted permanently after clicking "Accept" or alternatively "OK".

6.4.5.2 The "Export configuration file" menu option

By using the "Export configuration file" dialogue, it is possible to write the settings of the individual IKARUS security.manager instances to a new configuration file in an encrypted form. This file can then be forwarded at will. You can call the dialogue using the Management → Export configuration file menu.



Figure 77: UI - "Management" menu, "Export configuration file" menu option

Please note that the "Management" menu is not available in single mode.

The dialogue shows a list with all IKARUS security.manager instances as well as their key information. You can use the checkboxes on the left edge of the list to choose whether all instances or only specific ones are to be exported.

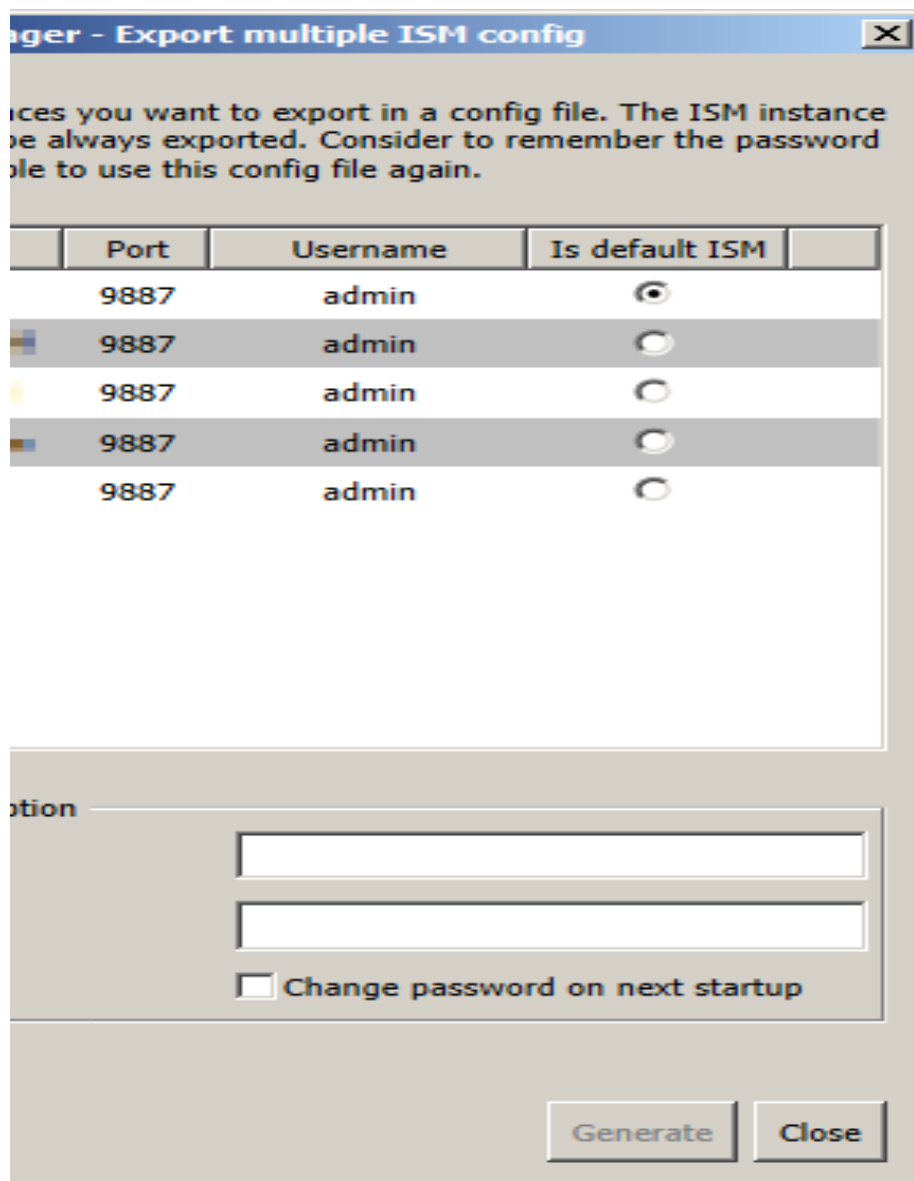


Figure 78: UI - "Export configuration file" dialogue - selecting the ISM instances to be exported

For security reasons, it is necessary to give a password before exporting the file. It is used to encrypt the file. You must enter it using the two text boxes under the list, and the entries must be identical.

Attention: The password must be at least 4 characters long, and you must enter that same value in both text boxes. You can only export the data when these conditions have been met.

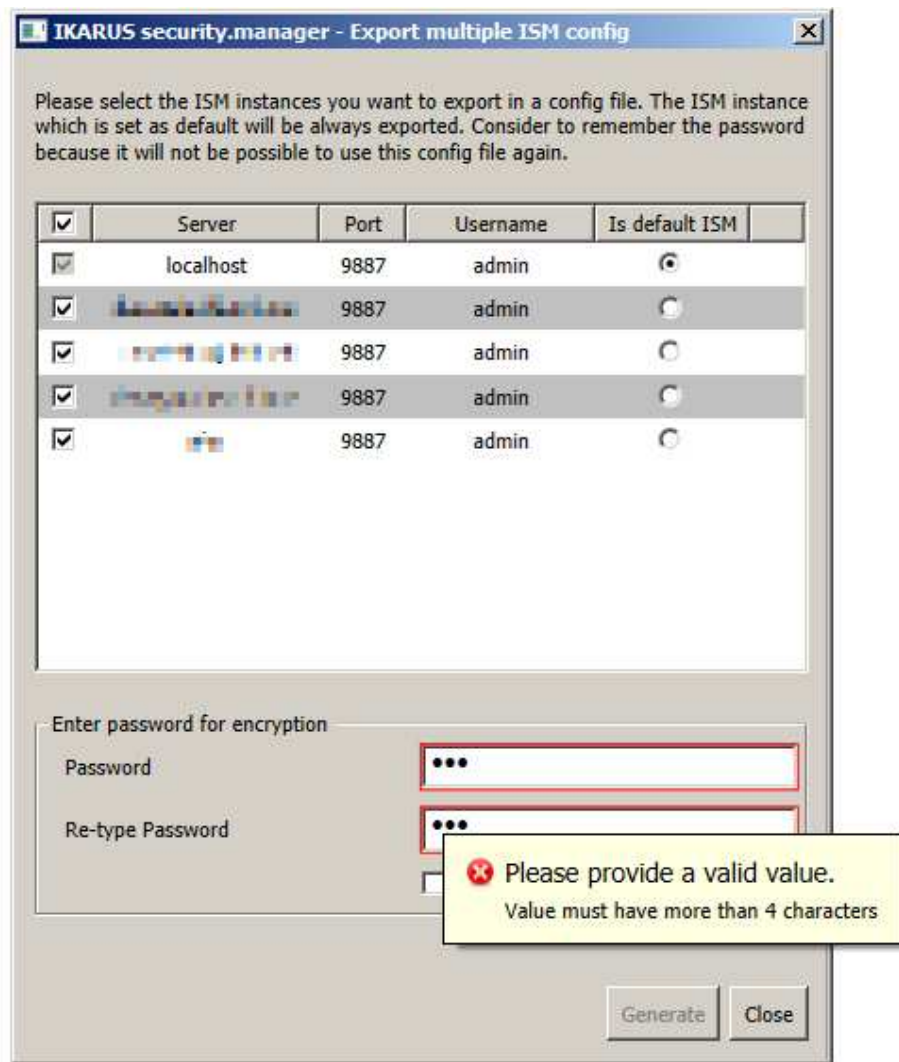
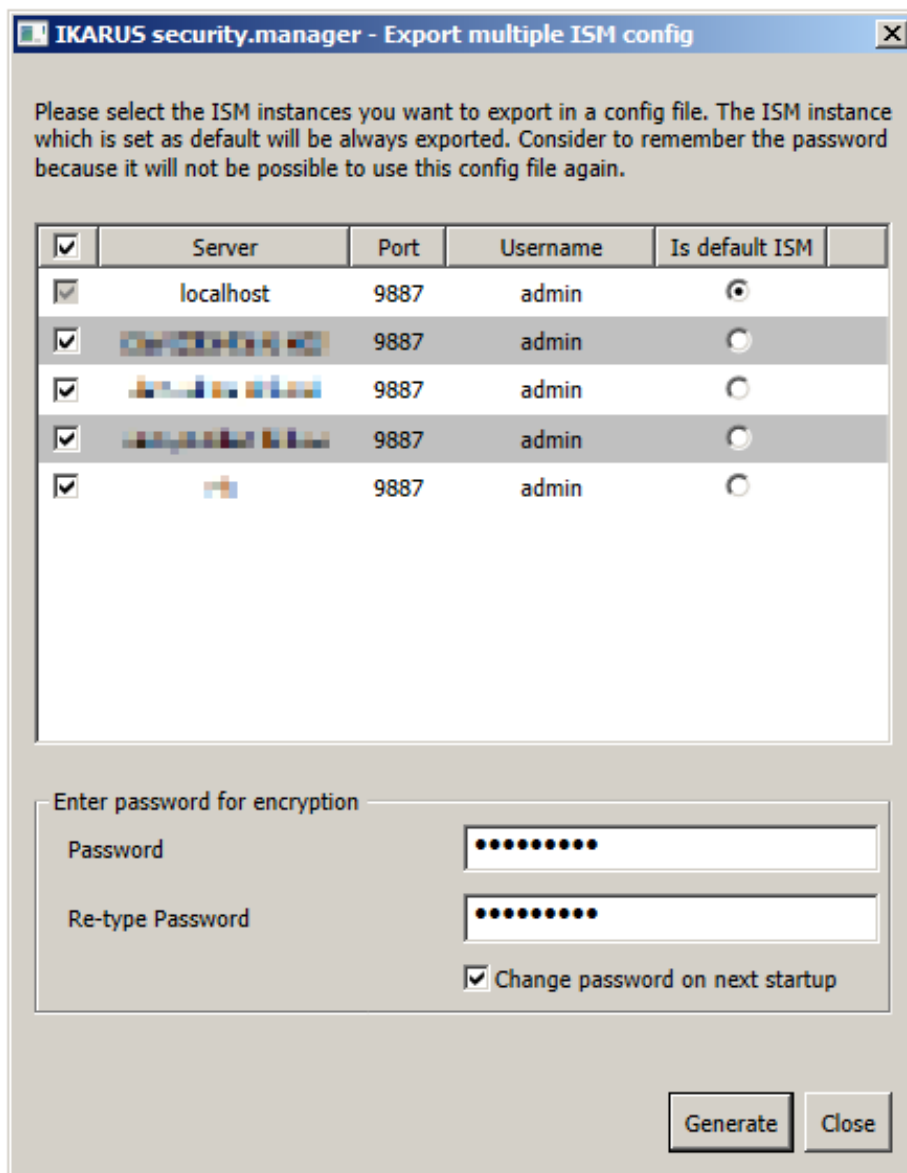


Figure 79: UI "Export configuration file" dialogue - error message in the event of an invalid password.

If you mark "Change password on next start-up", then the user who wants to use your exported file will be requested to reset the password for the encryption of the file when the program is started for the first time with your configuration file. Otherwise, the value that you set will be used for this.



Please select the ISM instances you want to export in a config file. The ISM instance which is set as default will be always exported. Consider to remember the password because it will not be possible to use this config file again.

<input checked="" type="checkbox"/>	Server	Port	Username	Is default ISM
<input checked="" type="checkbox"/>	localhost	9887	admin	<input checked="" type="radio"/>
<input checked="" type="checkbox"/>	[REDACTED]	9887	admin	<input type="radio"/>
<input checked="" type="checkbox"/>	[REDACTED]	9887	admin	<input type="radio"/>
<input checked="" type="checkbox"/>	[REDACTED]	9887	admin	<input type="radio"/>
<input checked="" type="checkbox"/>	[REDACTED]	9887	admin	<input type="radio"/>

Enter password for encryption

Password

Re-type Password

☒ Change password on next startup

Generate **Close**

Figure 80: UI "Export configuration file" dialogue - valid password

Now, you can start the export of the selected IKARUS security.manager instances by clicking "Generate". In the following dialogue, you will be requested to specify the storage path as well as a file name.

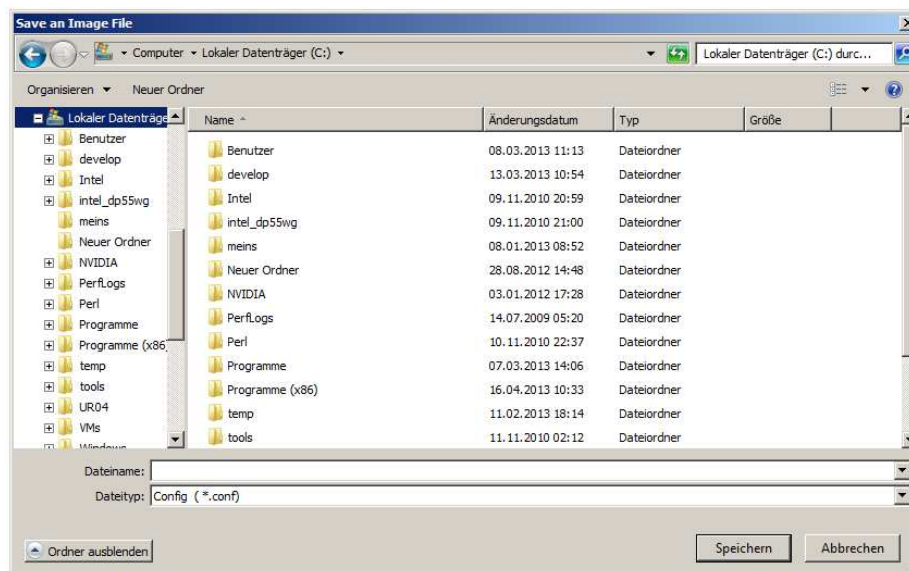


Figure 81: UI - Save file dialogue for exporting the configuration file

One click on "Save" saves the information in an encrypted form in the new file.

6.4.5.3 The "Change the password for management mode" menu option

This dialogue can be used to change the password for logging in to management mode. It is available under the Management menu option.

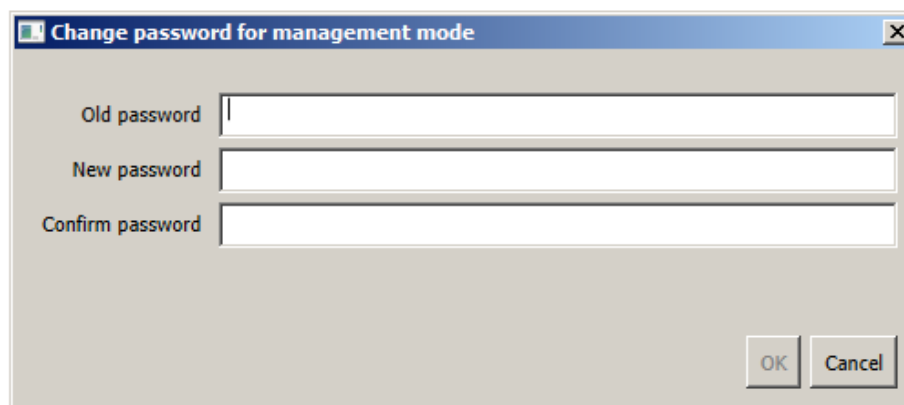


Figure 82: UI - Changing the password for management mode

It is important to note that password changes in management mode have no effect on the passwords of the registered IKARUS security.manager servers. These changes only affect the settings file that contains the list of registered IKARUS security.manager servers.

6.5 The Toolbar

The Toolbar (Figure 83) can be found at the top of the IKARUS security.manager UI main window right below the *Menu Bar*. The IKARUS anti.virus Configurations opens the IKARUS anti.virus Configurations window, see section 6.5.1 for more information.



Figure 83: UI – Toolbar

6.5.1 IKARUS anti.virus Configurations

The IKARUS anti.virus Configurations window (Figure 84) lists all available IKARUS anti.virus configurations and the [clients](#) that use them. You can edit a configuration by clicking the “Edit selected Configuration” button or by double-clicking the configuration you want to alter. For further information about the IKARUS anti.virus configuration and the various settings, refer to the IKARUS anti.virus manual.

6.5.1.1 Layout

In the toolbar of the Configurations dialog it is possible to do the following actions:

- Add Configuration
- Edit selected Configuration
- Delete selected Configuration
- Import Configuration
- Export selected Configuration

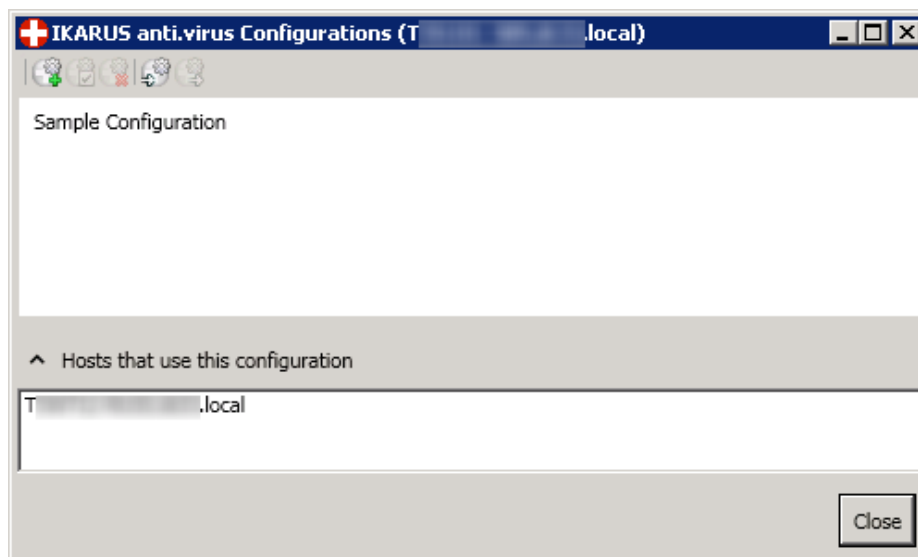


Figure 84: UI – IKARUS anti.virus Configurations

In the first list of the dialog all available configurations of the IKARUS security.manager are shown and by opening the second list, it is also possible to view all hosts that use the selected configuration.

6.5.1.2 General

On the General tab of the IKARUS anti.virus Configuration dialog, all necessary protection settings can be enabled or disabled. The configuration can be saved by clicking the OK or the Save button and the changes can be discarded by clicking the Cancel button. Clicking the OK or Cancel buttons will also close the IKARUS anti.virus Configuration dialog.

It is possible to set the following settings on the General tab:

- **Enable System Protection:**
Enables or disables system protection (if disabled, all other options will be disabled, too)
- **Enable Internet download protection:**
Enables or disables protection for Internet downloads
- **Enable spyware protection:**
Enables or disables spyware protection
- **Enable dialer protection:**
Enables or disables dialer protection

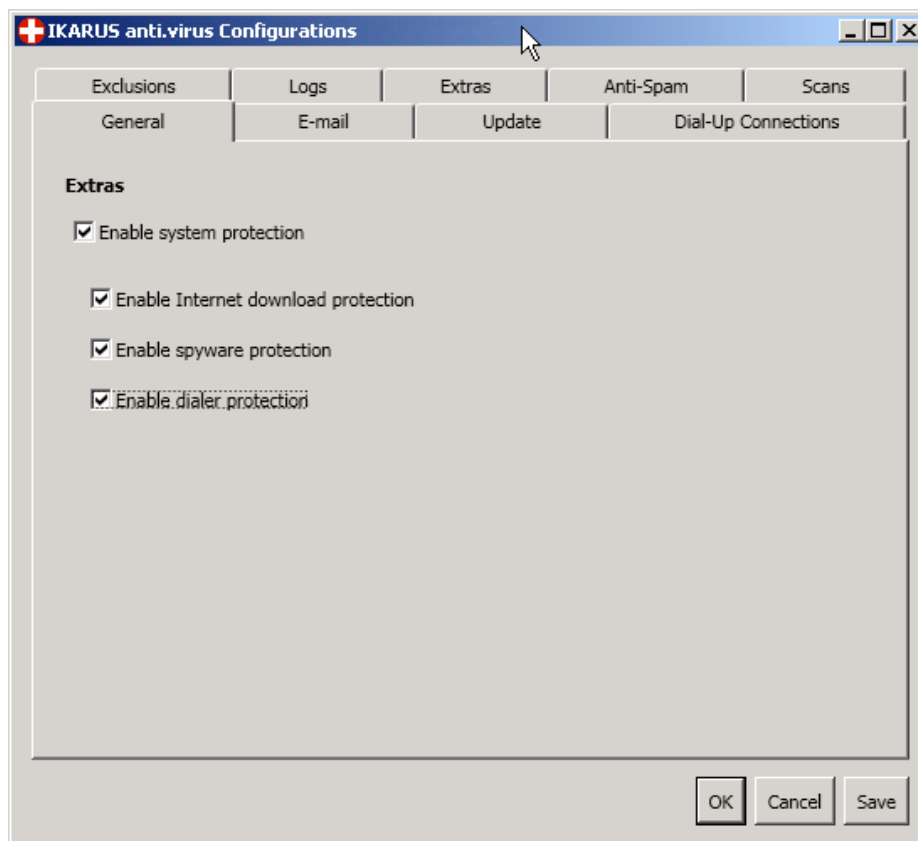


Figure 85: Configuration General Tab

6.5.1.3 E-mail

On the e-mail tab of the IKARUS anti.virus Configuration, e-mail protection of the client can be enabled or disabled. Additionally, the administrator can configure various settings such as where the scan report is placed in the e-mail. With incoming and outgoing e-mails, the e-mail scan report can be positioned at the beginning or the end of the e-mail or be omitted.

In the email section it is possible to configure the following settings:

- **Activate email Protection:**
Enables or disables e-mail protection
- **Save infected attachments:**
Specifies whether attachments should be saved on the client side
- **Show scan status:**
Shows the scan status
- **For incoming e-mails:**
Sets the position of the scan report in incoming mail
- **For outgoing e-mails:**
Sets the position of the scan report in outgoing mail

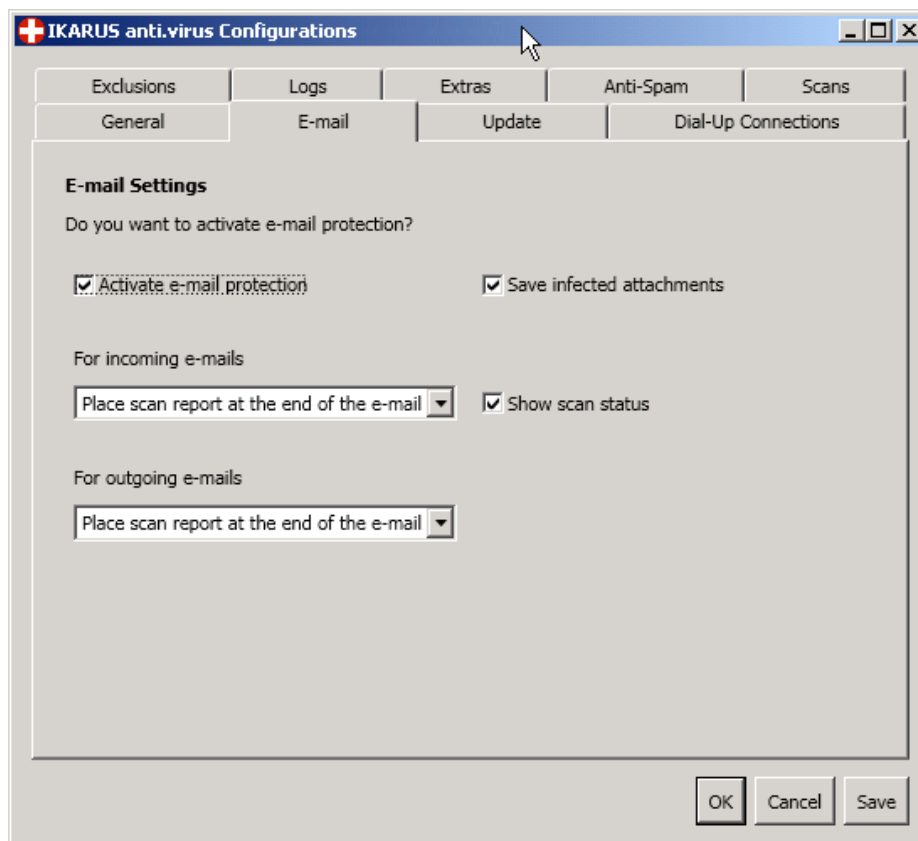


Figure 86: Configuration e-mail tab

6.5.1.4 Update

All settings necessary for updates to the IKARUS anti.virus are configured on the Update tab. In particular, when using a proxy server, you need to specify the correct settings here.

In the update tab the following settings can be set:

- Search automatically:
Enables automatic search
- Install product update automatically:
Automatically installs product updates
- Use proxy server:
Enables/disables use of a proxy server
- Server:
Proxy-server address
- Port:
Proxy-server port
- Username:
The username for the proxy server if needed

- Password:
The password for the proxy server if needed

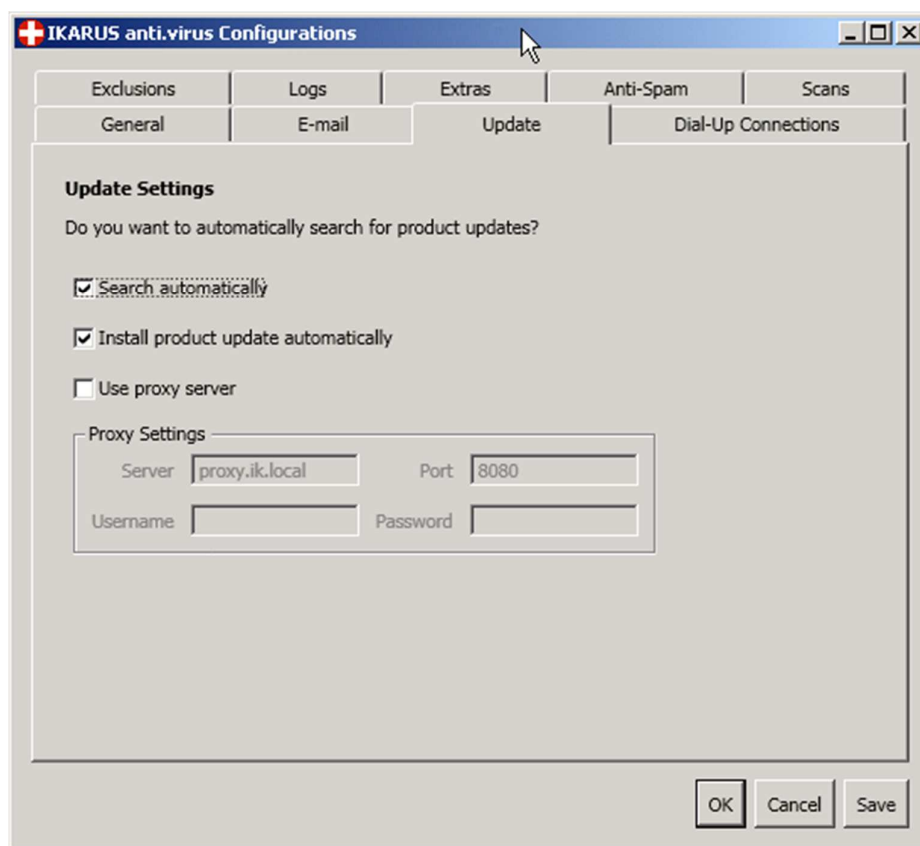


Figure 87: Configuration Update tab

6.5.1.5 Dial-Up Connections

If you still have a modem or dial-up connection in place you can set the connection settings on the Dial-Up Connections tab. The Modem connection tab allows for setting the auto-dial function for updating the IKARUS anti.virus. You can specify a period of time during which Auto Update will automatically connect to the Internet (if dial-up connection is selected).

In the dial-up tab the following settings can be adapted:

- Modem/Dial up connection:
Enter the dial-up or modem connection name here
- Activate automatic dialing:
Enables automatic dialing
- Timespan setting:
Sets the time frame when the connection is automatically established

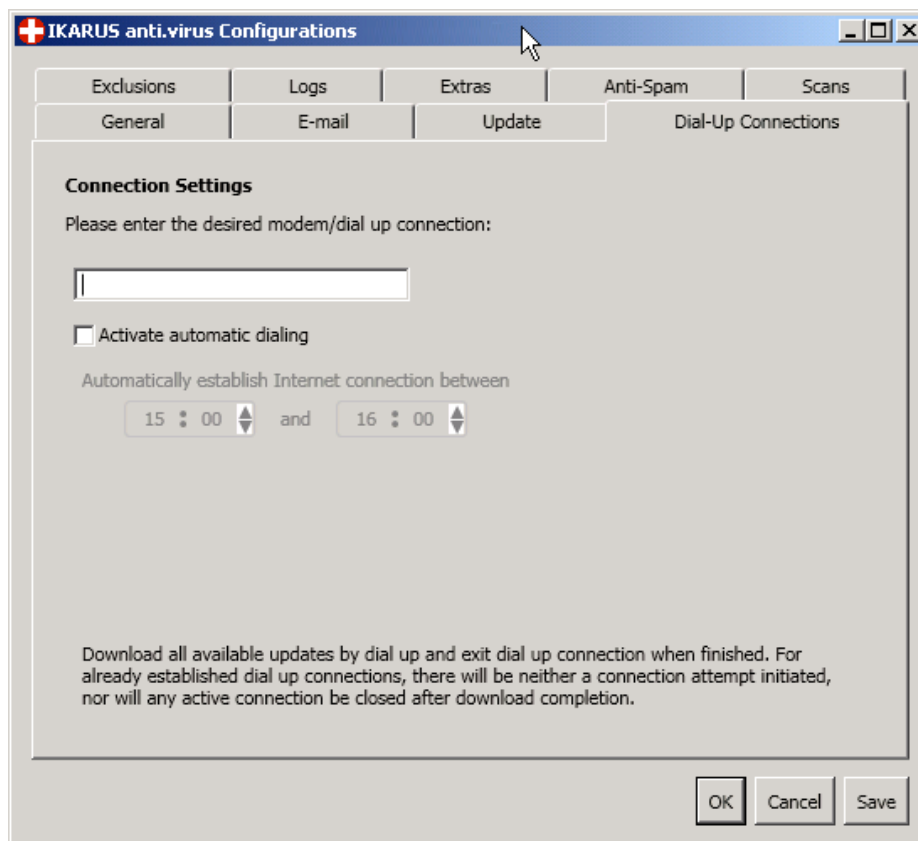


Figure 88: Configuration Dial-Up Connections tab

6.5.1.6 Exclusions

On the Exclusions tab, you can select files and process that will be excluded from the IKARUS anti.virus scan. This is useful when you want to exclude a service from the scan that is already using a considerable amount of the system resources (e.g. MP3, holiday photos, etc.), or if you do not want to scan a specific directory.

If you have set environment variables for specific folders/drives you want to exclude system-wide, use this function rather than specifying the path. If the path is different on every host, the IKARUS anti.virus will exclude the correct path. Use Ctrl + Spacebar in the textbox to display all environment variables of your current system (i.e. the system where the user interface is installed).

In the exclusion tab it is possible to configure the following settings:

- MiB number box:
Enables or disables file scanning for files bigger than the specified size.
- Add button:
Add paths and environment variables on the file exclusion tab.

- List of Exclusions:
This is a list of already selected paths/environment variables. If you choose the process exclusions it displays the excluded processes.
- Generalize Paths:
If you are not sure whether there is an environment variable for a path, click Generalize Paths. This link is not available for process exclusions.
 - ✓ Old Path:
The path you entered
 - ✓ New Path:
The path replaced with environment variables
 - ✓ Apply:
Check if you want to apply the change

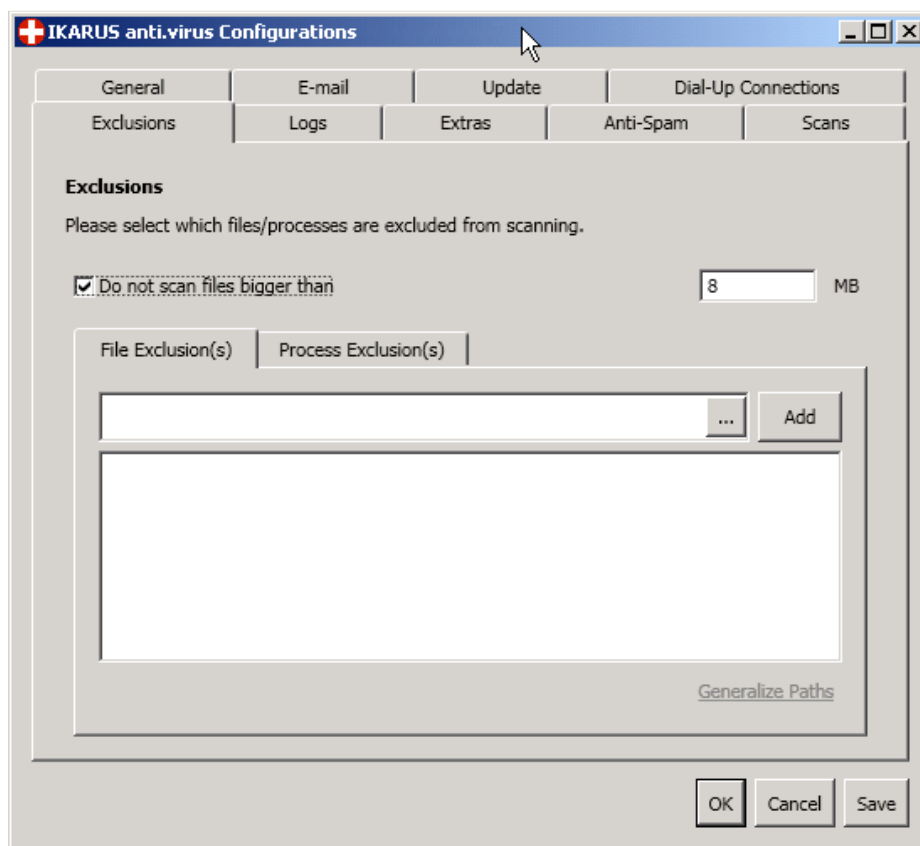


Figure 89: "IKARUS anti.virus-Configurations" Exclusion tab

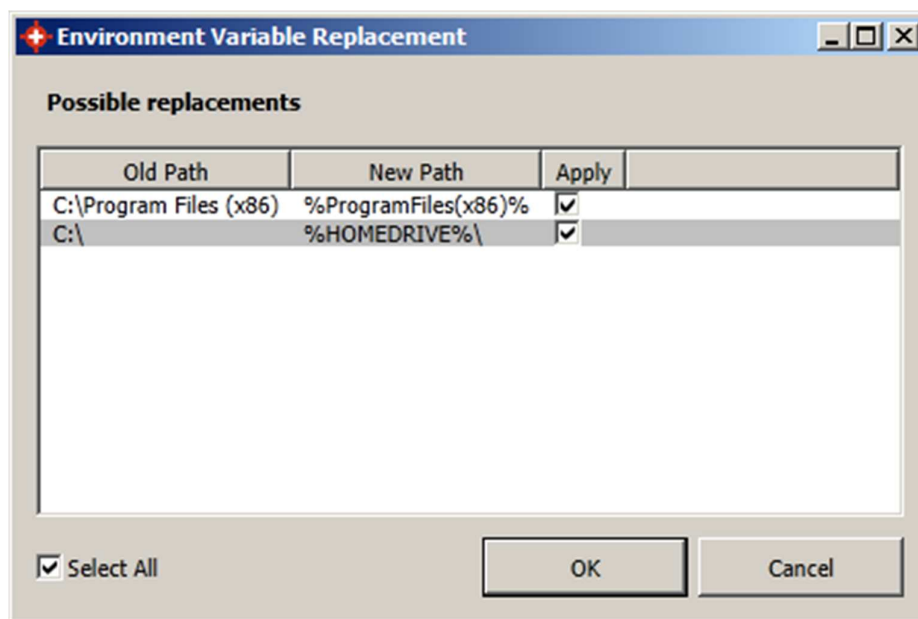


Figure 90: Configuration Exclusion tab (File exclusion)

6.5.1.7 Logs

On the Logs tab, the administrator defines actions that will be logged in the IKARUS anti.virus.

In the logs tab the following settings can be changed:

- Log system supervision in the main log:
Logs the system supervision to the IKARUS anti.virus main log.
- Record logs for scans:
Enable if logs should be written for the scans.
- Record all data when scanning:
Enable if all data should be recorded.
- Activate log file overwrite:
An existing log will be overwritten when a new scan is started.

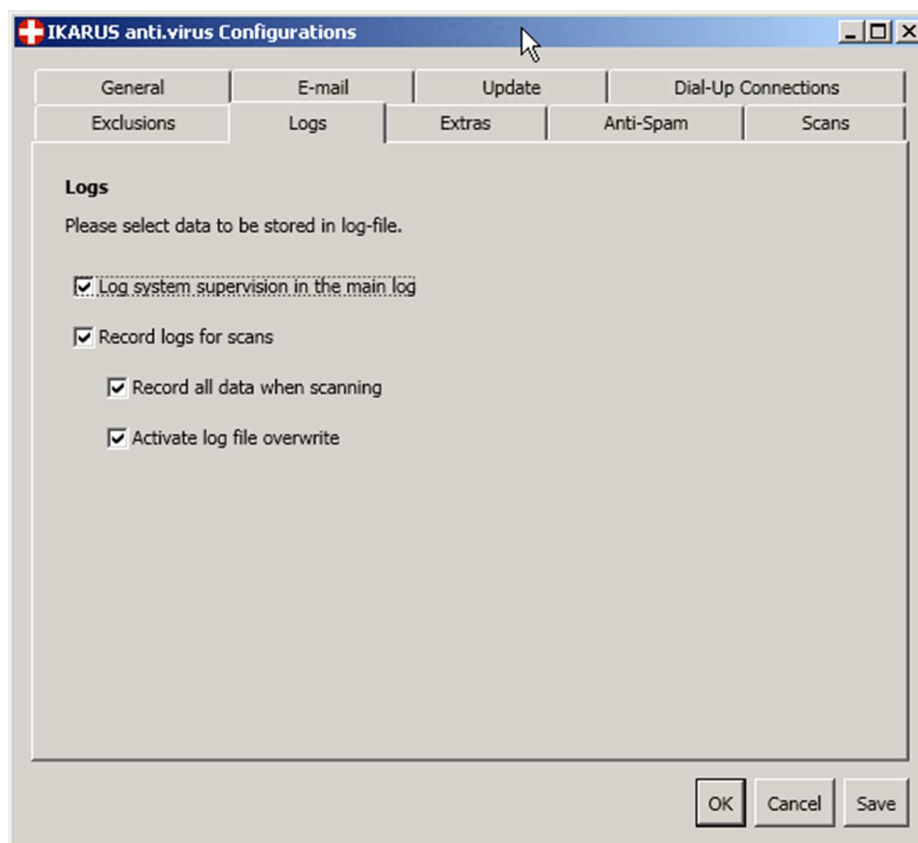


Figure 91: Configuration Logs tab

6.5.1.8 Extras

Use the Extras tab to restore the defaults of the IKARUS anti.virus and to enable system protection for the start-up processes of your operation system. In the Extras tab the system protection can be enabled to start at start-up and it is possible to reset all settings to the default configuration.

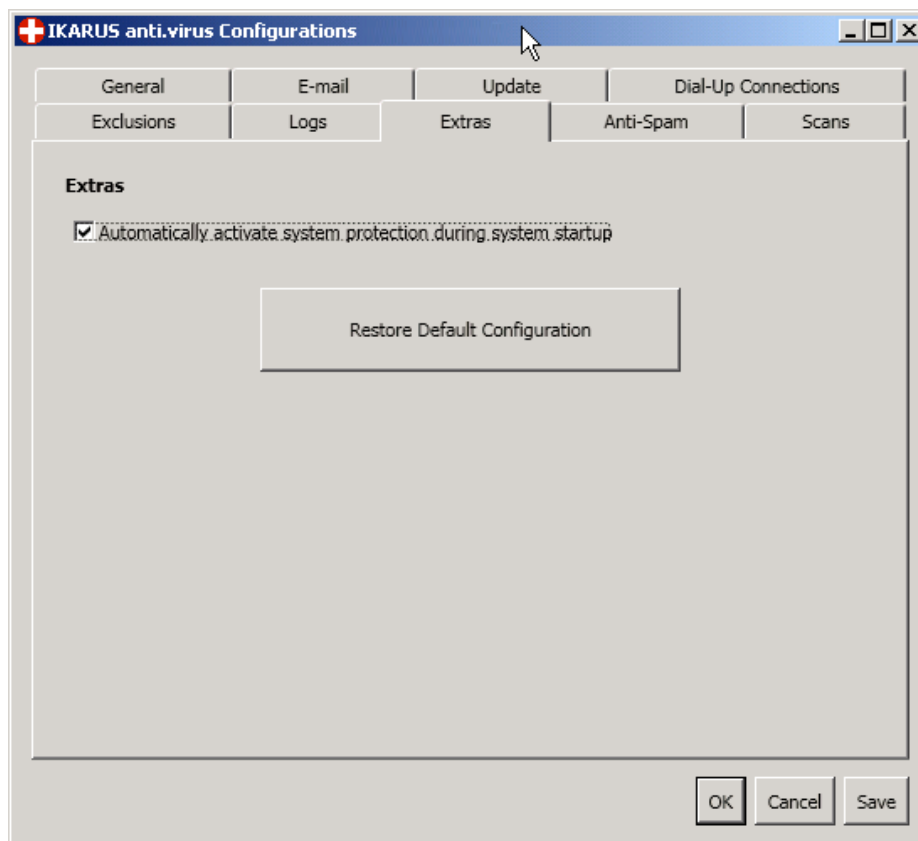


Figure 92: Configuration Extras tab

6.5.1.9 Anti-Spam

The IKARUS Anti-Spam Module allows for filtering e-mail received in Outlook, Outlook Express, or Windows Mail. Click the Activate Anti-Spam option in the settings of IKARUS anti.virus to enable spam protection.

The Anti-Spam Module will be enabled after the subsequent program restart. For configuring spam evaluation, click the yellow and red controls (yellow indicates possible spam, and red indicates spam).

At the bottom, you can choose the action to perform when receiving spam mail:

- Mark e-mail with a "Possible Spam" label in the subject line, or
- Move mail to the junk mail folder of your mail client

An e-mail that is considered as a possible spam, will always be labelled in the subject line but will remain in the inbox of your mail client.

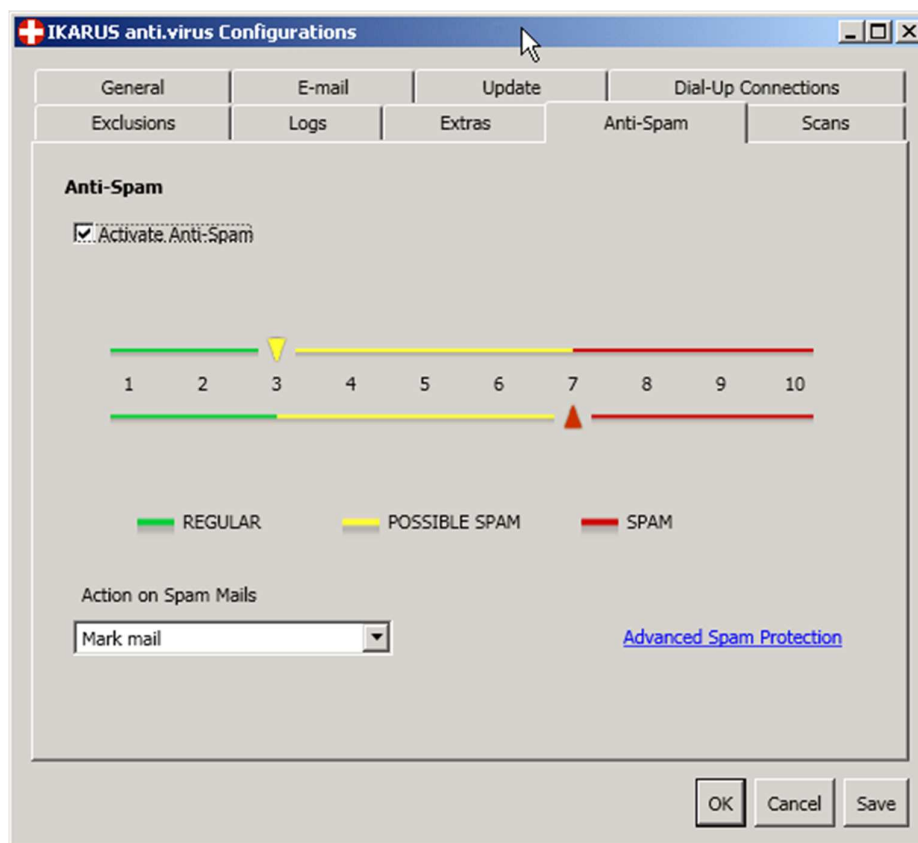


Figure 93: Configuration Anti-Spam tab

Advanced Spam Protection:

This option allows for configuring your own spam filter. You can define spam rules for senders, recipients, subjects, and contents.

The following settings can be made:

- E-mail Section:
Defines what section like sender, recipient, subject or content should be used for spam-rules
- Content:
Content to parse for
- Type:
Type of e-mail that can be regular mail, possible spam or spam
- Add button:
Click to enable advanced spam protection
- E-mail Section column:
List entry e-mail section
- Content column:
List entry content
- Type column:
List entry e-mail type

- Priority column:
By the help of these buttons the rules can be deleted or moved to new locations:
 - ✓ Delete Advanced Spam Protection
 - ✓ Move to Top
 - ✓ Move up
 - ✓ Move down
 - ✓ Move to Bottom

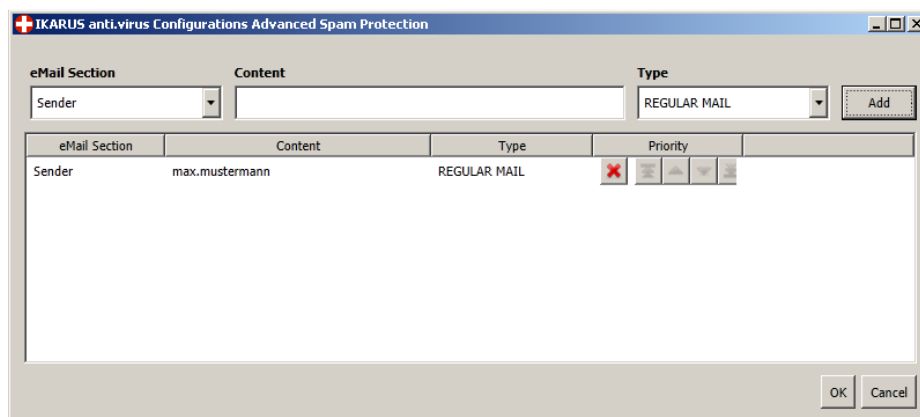


Figure 94: Configuration Advanced Spam Protection

6.5.1.10 Scan

You can configure the scan to be performed automatically or launch the scan manually in IKARUS anti.virus. You can manage and add as many scans as required.

Pre-set scans:

- Fast System Scan:
Scans the Windows installation directory. The majority of malicious programs such as viruses and Trojan horses are located in this directory and are quickly and reliably detected.
- System Partition:
This pre-set scans the drive where your operating system is installed. All archives, directories, folders, and files on this drive will be scanned by IKARUS anti.virus.
- Entire Host:
IKARUS anti.virus will scan all drives on your computer.
- Removable media:
All external drives such as USB sticks and CD ROM drives will be scanned.

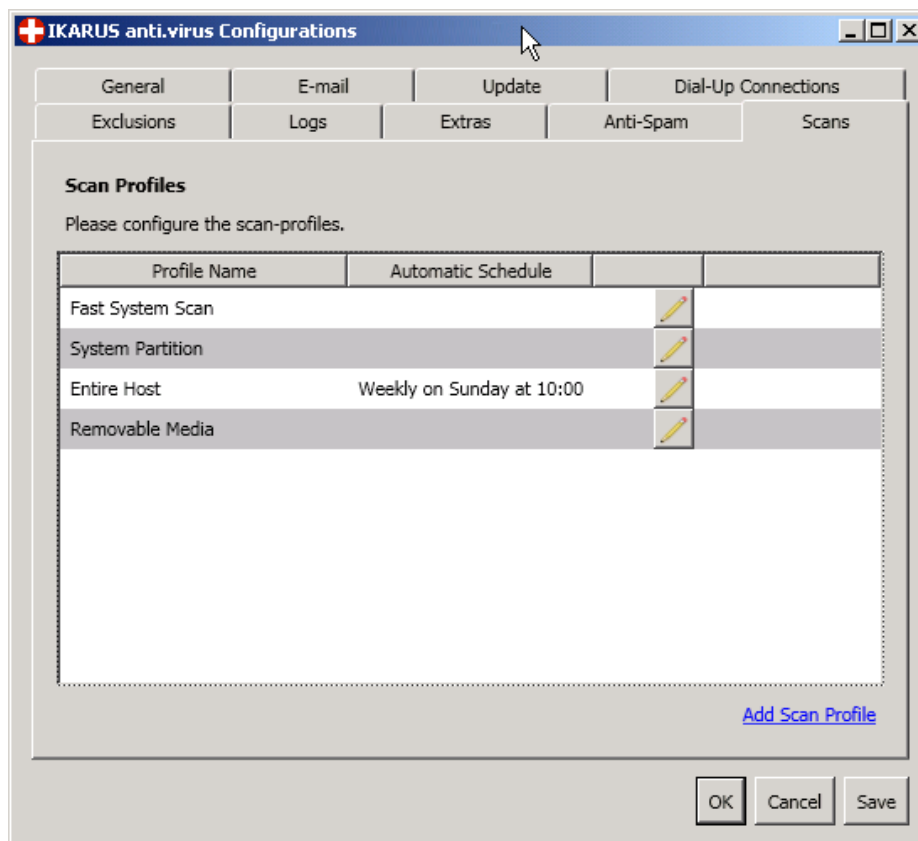


Figure 95: Configuration Scans tab

Click “Add Scan Profile” to configure a custom scan profile. You can enter any name for the scan. Click “Browse” to select the folders or files to scan. You can also set the program to perform an automatic scan where required.

The automatic scan can be scheduled for any time (for example, every Friday, 12pm). The scan will be performed only for those areas selected by the user.

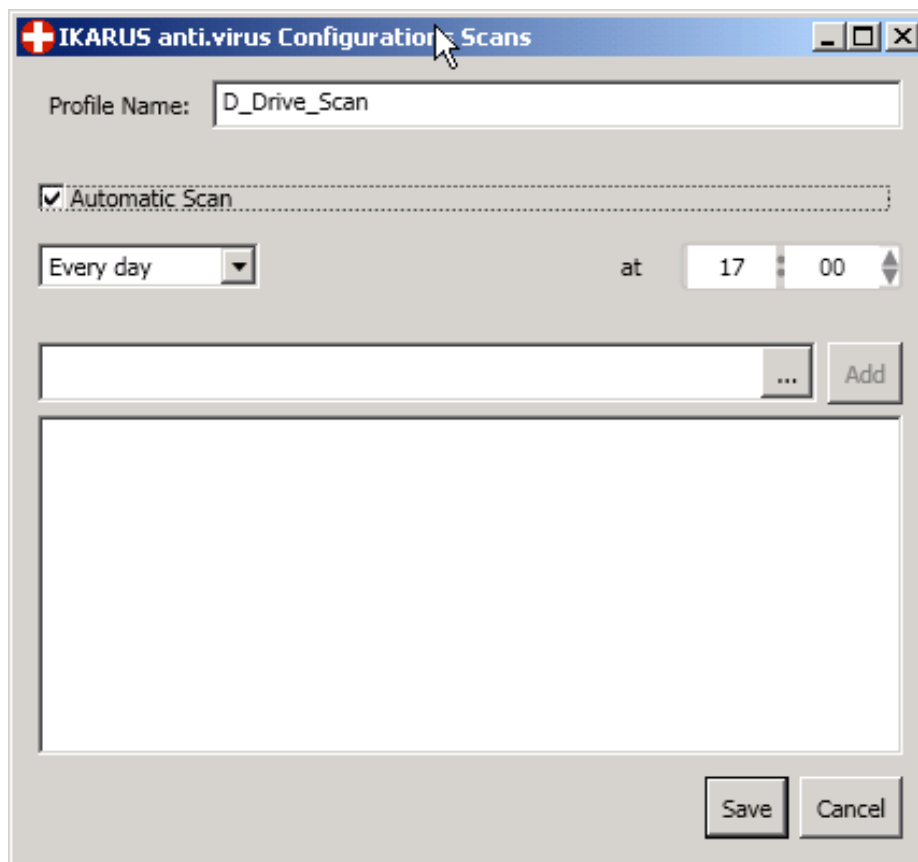


Figure 96: Configuration Add Scan Profile

6.6 Notification Bar

The Notification Bar control (Figure 97) is hidden by default. It will only be displayed if there have been changes to the virus list of a [client](#). If the IKARUS security.manager UI is not the active (foreground) application, the IKARUS security.manager UI entry in the Windows taskbar will start flashing to inform you that there are virus list changes.

6.6.1 Layout



Figure 97: UI – Notification Bar

7

The Shared Directory

The Shared Directory is the [network share](#) where the ismxstartup.exe file will reside. As this executable is required for installing the IKARUS anti.virus on a [client](#), that particular [client](#) needs read access to that share and file.

Further, the IKARUS security.manager Server needs write access to that [network share](#) to place the file on the share in the first place. You can specify the Shared Directory in the [General IKARUS security.manager Settings](#) dialog (see Figure 59). Please verify if it is possible to access the shared directory also from the host where the database is available and if the database user has write rights. During the creation of a database backup, it is necessary to write the generated backup file to the shared directory. This file will be automatically added to the support zip (see section 6.4.3) and afterwards from the shared directory removed.

8

Software Distribution

The installation and uninstallation processes for the IKARUS anti.virus are subdivided into different steps. To complete these steps successfully, the following criteria must be met:

- The IKARUS security.manager Server needs a [shared directory](#) (see Figure 59) set to place the binaries needed for a remote installation.
- The IKARUS security.manager Server needs appropriate rights to remotely execute binaries on the target [client](#). If the IKARUS security.manager Server has been installed with a [domain](#) administrator account and the target [client](#) is on the same [domain](#) as the IKARUS security.manager Server, no further adjustments need to be made for that [client](#); otherwise, you need to specify credentials having appropriate rights to launch executable files on the target [client](#). You can configure this on a client's [Rights Management](#) tab on the IKARUS security.manager UI.
- The target [client](#) needs at least read access to the user-defined [shared directory](#) to retrieve the ismxstartup binary.
- The [TCP](#) communication ports need to be forwarded when using a firewall.
- The target [client](#) must meet the hardware and software requirements specified to operate the IKARUS anti.virus. Refer to the requirements indicated in the IKARUS anti.virus manual.
- The Enforce Client Update option in the [IKARUS security.manager Settings](#) windows (Figure 59) must be enabled.

8.1 Installing the IKARUS anti.virus

To install and deploy the IKARUS anti.virus, right-click a [client](#) or group in the [Directory](#) to open the context menu and click on the Install anti.virus entry. The installation of the IKARUS anti.virus includes the below steps (Figure 98). It can take a moment, so please wait patiently:

- Step 1:
The IKARUS security.manager Server places the needed executable files in the [Shared Directory](#).
- Step 2:
The IKARUS security.manager Server tries to install the ismxstartup [service](#) remotely from the [Shared Directory](#). The target [client](#) needs read access to the [Shared Directory](#) and to files in it.

- Step 3:
The ismxstartup [service](#) retrieves the guardxup binary from the IKARUS security.manager Server, places it into the Windows temp directory of the target [client](#), and launches it.
- Step 4:
The guardxup binary performs all further steps left for installing the IKARUS anti.virus on the target [client](#). This includes retrieving the IKARUS anti.virus binaries from the IKARUS security.manager Server and installing them on the target.

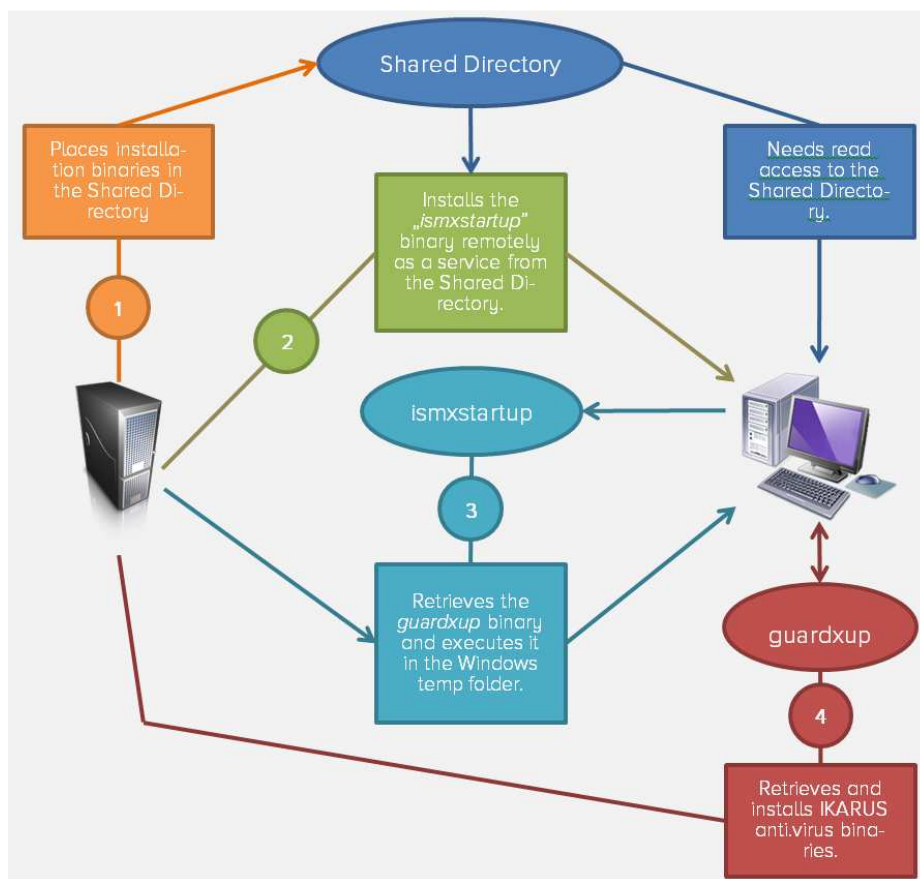


Figure 98: Software Distribution – Installation process

8.2 Uninstalling the IKARUS anti.virus

To uninstall the IKARUS anti.virus, right-click the [client](#) or group of the [Directory](#). In the opening context menu, click the Uninstall anti.virus item.

Note: Uninstallation can be done for [administered clients](#) only.

9

Configuration file

The Configuration File (named ism.conf) exists in the conf directory of the installation destination which will be chosen when installing the IKARUS security.manager Server (see section 0). The [MSSQL](#)-database connection information as well as the [LDAP](#) connection settings and the [TCP](#) ports used for the communication between the IKARUS anti.virus and the IKARUS security.manager are configured by this file.

Sample Config file:

```
<config>
  dbconnstring DRIVER={SQL Server};SERVER=localhost
  serverport    9887
  clientupdateport  9888
  timespanAD    12
</config>

<ldap>
  type    native
  servername    esx-2k8-de-srv.labor.local
  searchpath    dc=labor,dc=local
  authmethod    simple
  username      LDAP Connector
  password      none
  attribute      dNSHostName
  filter (objectCategory=computer)
</ldap>
```

Note: It is possible to edit [LDAP](#) parameters by the help of the IKARUS security.manager settings within the IKARUS security.manager UI. For further information please check section 6.4.3.2.5.

9.1 The <config> Section

In the <config> section, you can provide information about the [MSSQL](#) database used by the IKARUS security.manager Server for storing data and information and about the [TCP](#) ports used for communication. Furthermore it is possible to set the scheduled time or timespan, when the [Active Directory](#) should be refreshed in the IKARUS security.manager Server.

Setting	Description
dbconnstring	The information used for establishing a connection to the target MSSQL database. Includes the server name where the database resides and authentication methods needed for accessing the database. For more information about the syntax and available properties of the connection string, refer to your MSSQL documentation.
serverport	The TCP port used for the communication between the IKARUS security.manager Server and the IKARUS security.manager UI. If you use a firewall , make sure to forward this port.
clientupdateport	The TCP port used for the communication between the update binaries and the IKARUS anti.virus. If you use a firewall , make sure to forward this port.
timespanAD	Allows values between 1 and 24, which means that from the time, when the value was provided (or the server was restarted), every X hours the Active Directory is reloaded. The default setting for reloading the AD is internally set to "every 12 hours". This setting always overrules, if set in the config file, the daytimeAD setting.
daytimeAD	Allows values between 0 and 23, which means that every day at the given time the AD is reloaded. It is not possible to use this setting together with the timespanAD setting. The timespanAD setting, if set, always overrules the daytimeAD setting.

Table 5: Possible settings for <config>

9.2 The <ldap> Section

The <ldap> section includes information about the [LDAP server](#) the IKARUS security.manager Server connects to resolve the [clients](#) existing in your [active directory](#). If no <ldap> section is found in the [config file](#), the IKARUS security.manager Server will try to obtain the information from the [domain controller](#).

Setting	Description
type	The type of the LDAP configuration.

servername	The name of the domain controller .
searchpath	Specifies the domains to scan. Domain levels are split with the dc (Domain component) keyword. Example for a .company.local domain: searchpath dc=company dc=local
authmethod	Describes the method used for authenticating with the domain controller . If you do not want to authenticate with a specific user, specify anonymous here.
username	Sets the username used for authenticating with the domain controller . Only required if the authentication method is not set to anonymous.
password	Sets the password used for authenticating with the domain controller . Only required if the authentication method is not set to anonymous.
attribute	Sets the attribute to read.
filter	Sets the criteria used on resolving the specified attribute.

Table 6: Possible settings <ldap>

10

Glossary

Abbreviation	Term	Description
	IKARUS anti.virus	IKARUS anti.virus, our award-winning virus protection for workstations and server allows you to identify, detect and delete all kinds of malware.
	Windows service	A Windows service is an executable designed for running in the background without user interaction. Windows services can be set up to automatically start at boot time. Windows services can be installed either using a user account available on your Windows network or a local service account.
MSSQL	Microsoft Structured Query Language	Microsoft SQL Server is a relational database server developed by Microsoft. Its primary function is to store and retrieve data as requested by other software applications running on the same computer or a different computer on a network (including the Internet).
TCP	Transmission Control Protocol	The Transmission Control Protocol is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite and complements the Internet Protocol . Therefore, the entire suite is commonly referred to as TCP/IP. TCP provides reliable ordered delivery of a byte stream from a program on one computer to another program on a different computer.
IP	Internet Protocol	The Internet Protocol is the principal communication protocol used for relaying datagrams (packets) across an internetwork using the IP Suite. It allows for routing packets across network boundaries and is the primary foundation of the Internet .
LDAP	Lightweight Directory Access Protocol	LDAP is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol network.

	Proxy Server	In computer networks, a proxy server is a server (i.e. a computer system or an application) acting as an intermediary for requests from clients seeking resources from other servers .
	Network share	In computing, a shared resource or network share is a device or piece of information on a computer that can be remotely accessed from another computer, typically on a local area network or an enterprise intranet . The access is transparent: There is no difference between accessing a local or remote resource.
LAN	Local Area Network	A local area network is a computer network that interconnects computers in a specific area such as a home, a school, a computer laboratory, or an office building.
	Intranet	An intranet is a computer network that uses Internet Protocol technology for securely sharing any parts of an organization's information or network operating system within that organization.
AD	Active Directory	The Active Directory is a directory service developed by Microsoft for Windows domain networks. It is part of the most Windows Server operating systems. Server computers running Active Directory are referred to as domain controllers .
	Windows domain	A Windows domain is a collection of security principals sharing a central directory database. This central database (known as Active Directory starting with Windows 2000 ^[1] , Active Directory Domain Services in Windows Server 2008 and Server 2008 R2, also referred to as NT Directory Services on Windows NT operating systems, or NTDS) holds the user accounts and security information for resources in that domain. Each person who uses computers in a domain gets a unique account or user name. This account can then be assigned access to resources within the domain.
	Directory Service	A directory service is the software system that stores, organizes and provides access to information in a directory. In software engineering, a directory is a map between names and values. It allows for looking up values associated with a name; this is similar to a dictionary.
DC	Domain Controller	On Windows Server systems, a domain controller is a server handling security authentication requests (logins, permissions checks, etc.) in the Windows Server domain . A domain is a concept introduced with Windows NT that

		grants a user access to a number of computer resources if he or she can provide a combination of a username and password.
	Server	In the context of client-server architectures, a server is a computer program serving the requests of other computer programs named clients . The means that the server performs computational tasks on behalf of clients . The clients either run on the same computer or connect through a network.
	Client	A client is an application or system that accesses a service made available by a server . The server typically (but not always) exists on a different computer system. In that case, the client accesses the service over the network.
FQDN	Fully Qualified Domain Name	A fully qualified domain name, sometimes also referred as an “absolute domain name”, is a domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). The FQDN includes all domain levels including the top-level domain and the root zone . A fully qualified domain name is distinguished by its unambiguity; it can only be interpreted one way.
	Domain Name	A domain name is an identification string that defines a scope of administrative autonomy, authority, or control on the Internet. Domain names are formed according to the rules and procedures of the Domain Name System (DNS) .
DNS	Domain Name System	The Domain Name System is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various pieces of information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans to the numerical identifiers associated with networking equipment for the purpose of locating and addressing those devices worldwide.
TLD	Top-Level Domain	A top-level domain is a domain at the highest level in the hierarchical Domain Name System (DNS) . Top-level domain names are installed in the root zone of the name space. For all subordinate domains, the top-level domain is the last part of the domain name , that is, the last label of a fully qualified domain name .
	Root Zone	A root zone is the top-level DNS zone in a hierarchical namespace using the Domain Name System (DNS) . The term typically refers to the root zone of the largest global

		network, the Internet.
	DNS Zone	A DNS zone is a part of a domain name space using the Domain Name System (DNS) , for which administrative responsibility has been delegated.
	IKARUS Activation Key	
	Administer	In the context of the IKARUS security.manager, administration means that a client with the IKARUS anti.virus installed is managed by the IKARUS security.manager: The client gets updates, configurations, licenses and settings from the IKARUS security.manager. If a client is not administered, only status information will be displayed. The limit of clients you are allowed to administer is specified in the license you are using.
	Application (Software)	Application software, also known as an application or an “app”, is computer software designed to help the user to perform specific tasks.
	Computer Software	Computer software, or just software, is a computer programs with its related data providing instructions for telling a computer what to do and how to do it. In other words, software is a conceptual entity, which is a set of computer programs, procedures, and associated documentation concerned with the operation of a data processing system.
	Firewall	A firewall is a device or set of devices designed to permit or deny network communication based upon a set of rules. Firewalls are typically used for protecting networks from unauthorized access while permitting legitimate communications.
	ZIP	ZIP is a file format used for data compression and archiving. A zip file contains one or more files that have been compressed, to reduce file size, or stored as is.

Table 7: Glossary

11

Contact

IKARUS Security Software GmbH

Blechturm-gasse 11
1050 Vienna
Austria

Phone: +43 (0) 1 58995-0
Fax: +43 (0) 1 58995-100

office@ikarus.at
www.ikarussecurity.com

IKARUS Security Software Support Contact

Phone: +43 (0) 1 58995-400
Support times: Mon-Thu: 8.00 – 18.00 (CET)
Fri: 8.00 – 15.00 (CET)
E-Mail: support@ikarus.at

IKARUS Security Software Sales Contact

Phone: +43 (0) 1 58995-500
E-Mail: sales@ikarus.at